Draft NISTIR 7924

Reference Certificate Policy

Harold Booth
Andrew Regenscheid

National Institute of
Standards and Technology
U.S. Department of Commerce

Draft NISTIR 7924

Reference Certificate Policy

Harold Booth
Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

April 2013

U.S. Department of Commerce
Rebecca Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Interagency or Internal Report 7924
82 pages (April 2013)

Public comment period: *April 11, 2013* through *June 7, 2013*

National Institute of Standards and Technology

Attn: Computer Security Division, Information Technology Laboratory

100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

nistir7924-comments@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems.

Abstract

The purpose of this document is to identify a baseline set of security controls and practices to support the secure issuance of certificates. This baseline was developed with publicly-trusted Certificate Authorities (CAs) in mind. These CAs, who issue the certificates used to secure websites and sign software, play a particularly important role online. This document formatted as a Reference Certificate Policy (CP). We expect different applications and relying party communities will tailor this document based on their specific needs. It was structured and developed so that the CP developer can fill in sections specific to organizational needs and quickly produce a suitable CP. This Reference CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practices Framework.

Keywords

certificate authority; certificate policy; digital certificate; public key infrastructure

Acknowledgments

The authors wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. In particular, the authors appreciate the contributions of the Federal PKI's Certificate Policy Working Group, whose "X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework" document was the basis for many sections in this document.

Table of Contents

List of Appendices

Foreword

Background

Certificate Authorities (CAs), and the infrastructure they support, form the basis for one of the primary mechanisms for providing strong assurance of identity in online transactions. The widely placed trust in CAs is at the heart of security mechanisms used to protect business and financial transaction online. Notably, protocols such as Transport Layer Security (TLS) rely on CAs to identify servers and clients in web transactions. Governments around the world rely on CAs to identify parties involved in transactions with them.

However, recent high-profile security breaches at major CAs trusted by widely used operating systems and browsers have highlighted both the critical role CAs play in securing electronic transactions, as well as the need to strongly protect them from malicious attacks. Analyses have revealed that these security breaches were often the result of insufficient security controls being in place on the computer systems and networks at these CAs, and sometimes exacerbated by weak record keeping. Third-party auditing programs, whose role it was to verify that proper security controls were in place, were not sufficient to identify these lapses in security.

The purpose of this document is to identify a baseline set of security controls and practices to support the secure issuance of certificates. In particular, the baseline has been developed with publicly-trusted CAs in mind. These CAs, who issue the certificates used to secure websites and sign software, play a particularly important role online.

Reference Certificate Policy

This baseline set of controls has been written in the form of a "certificate policy." As defined by ITU Recommendation X.509, a "certificate policy" is "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements." That is, a certificate policy, or CP, defines the expectations and requirements of the relying party community that will trust the certificates issued by its CAs. The governance structure that represents the relying party is known as the Policy Authority. The Policy Authority is responsible for identifying the appropriate set of requirements for a given community, and oversees the CAs that issue certificates for that community.

In particular, this document was developed as a reference certificate policy. We expect different applications and relying party communities will tailor this document based on their specific needs. It was structured and developed so that the CP developer can fill in sections specific to organizational needs and quickly produce a suitable CP. This Reference CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practices Framework [RFC3647].

The United States Government's Federal PKI Common Policy was used as a base document for this reference certificate policy. The FPKI Common Policy is widely recognized for clearly articulating the requirements for certificate issuance for the certificates covered by this set of policies, which are primarily used by government entities to authenticate to government systems. Within this reference certificate policy, we've adapted the US Government's requirements to be more appropriate to the wider PKI community. We also significantly updated the requirements in the computer, lifecycle and network security control sections.

Originally conceived of as primarily offline systems, the architecture of large, modern CAs has

increasingly moved online. Registration Authorities (RAs), the part of the CA infrastructure that validates identities of subscribers, communicate with subscribers and CAs over the Internet, and CAs frequently issue certificates, based on the identity-proofing by RAs, through automated processes. This change in architecture, along with the changing threat environment faced by online systems, necessitates additional security mechanisms in place at CAs. The CA community has long recognized the need for tight physical security and key management at CAs, but these security controls must also be accompanied by computer, lifecycle and network security controls of appropriate strength.

Using this Document

This document is designed to be used as a template and guide for writing a CP for a specific community. The controls identified in this reference CP were intended to be appropriate for large, publicly-trusted CAs that issue certificates used to TLS and code signing. While most material in this document should be appropriate for a wide range of applications, each community will need to tailor the specific controls identified by their CP as appropriate. This may involve adding and removing material from this reference CP as needed to accommodate the needs and constraints for their particular application, as well as modifying the controls as necessary to meet the assurance level required by the relying party community.

To help guide the CP writer, there are three types of information in this reference CP: suggested text, fill-in fields, and instructions. A section may contain any or all of these types of information.

Suggested text: Most of the document is of this type. This text has been written to use without alteration. It represents a reasonable level of assurance for certificate issuance. The requirements reflect best business practice. However, the CP developer must consider his own organization's needs, resources, and capabilities carefully to ensure that all of the requirements, both those on the CA and on the organization itself, are adequate and can be met. Where appropriate, the suggested text can be altered, or can be replaced using the existing suggested text as an example.

Fill-in fields: Some sections of the document contain fields where choices must be made by the CP writer, to tailor it for the intended purpose. These fields are denoted by <angle brackets>, and will contain an indication of the type of information that is to be filled in. In some cases, the brackets will also contain a suggestion for the value to be filled in. The information supplied by the CP writer is intended to replace the fill-in field, including angle brackets.

Instruction: There are a few areas of the CP that cannot be predicted and do not lend themselves to suggesting a generalized best practices requirement, nor are they such that a simple number must be selected. In this case, a paragraph will be supplied, that begins with an Instruction: tag and is in italic typeface. The instruction will give the CP writer information about how to complete the section, using existing organizational policy or documentation, or by creating other technical documents that will be referenced in the CP. These paragraphs are intended to be removed once the CP is completed.

A primary objective for writing this document as a reference CP is to encourage better security practices for CAs. The as-is text is generally more detailed than a typical CP, particularly in areas such as network security. Compliance audits of CPSs against CPs based on this reference will serve to drive CA practices to a more secure, yet fully achievable, level.

1 Introduction

This document is intended to assist developers of Certificate Policies (CP) that are intended to control the issuance and management of public key certificates for specific organizations or applications. It is also intended to provide baseline requirements for secure certificate issuance, with special attention to network security best practices.

It has been written as a reference Certificate Policy, so that the CP developer can fill in sections specific to organizational needs and quickly produce a suitable CP. This Reference CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practices Framework [RFC3647]. The recommendations are intended to support audit programs.

Instruction: For the actual CP, remove the paragraphs above and replace it with a description of the Subscribers, organization(s), or application(s) that drive the requirements for certificate issuance that are defined in the CP.

A PKI that uses this CP may provide some or all of the following security management services:

- Key generation/storage
- Certificate generation, modification, re-key, and distribution
- Key escrow and recovery of private keys associated with encryption (e.g. key management, key establishment) certificates
- Certificate revocation list (CRL) generation and distribution
- Directory management of certificate related items
- Certificate token initialization/programming/management
- System management functions (e.g., security audit, configuration management, archive.)

This policy does not presume any particular PKI architecture. The policy may be implemented through a hierarchical PKI, mesh PKI, or a single Certification Authority (CA). A conforming infrastructure may be either commercially operated or government operated. CAs that issue certificates under this policy may operate simultaneously under other policies. CAs must not assert this policy in certificates unless they are issued in accordance with all the requirements of this policy.

1.1 Overview

A CA is a collection of hardware, software, personnel, and operating procedures that issue and manage public key certificates. The digital certificate binds a public key to a named subject. This allows relying parties to trust signatures or assertions made by the subject using the private key that corresponds to the public key contained in the certificate.

A fundamental element of modern secure communications is establishing trust in public keys. This begins with a Relying Party obtaining a Subscriber's public key certificate that is issued by a trusted entity certifying that the public key belongs to that Subscriber. Subscriber certificates that are not trusted directly may become trusted through successive validation of a chain of CA certificates from the Subscriber's certificate to a trust anchor (typically a Root-CA public key). Trust anchors are explicitly trusted by Relying Parties. Relying parties are responsible for securely obtaining trust anchors and for securely managing their trust anchor store. Relying parties, including the Trust Anchor Managers should configure trust anchors with great caution and should give full consideration to the requirements of this CP and associated compliance annual audit requirements.

1.2 Name and Identification

Instruction: Policy OIDs are identifiers in certificates that indicate the assurance provided by a certificate for a particular purpose. Relying parties use these OIDs to decide whether to rely on these certificates. Unless there is a pre-approved OID available, the governing policy authority must register an OID for the purpose of identifying the application-specific Certificate Policy. Once registered or approved, the OID shall be listed in this section of the CP.

1.3 PKI Participants

This section identifies roles that are relevant to the administration and operation of CAs under this policy.

1.3.1 PKI Authorities

Instruction: In a canonical organizationally monolithic PKI, the certification authority is an absolute authority for the assertion of attributes related to subscribers. Trust in such a CA derives from the fact that the CA is the embodiment of PKI policy for the organization. Few real-life organizations fit the textbook mold, however, and non-organizational PKIs can be a mishmash of authority, liability, and application. Therefore, rather than defining the CA as the only PKI authority, this section defines a number of authorities, designed to deconstruct the types of authorities that would typically be held by a CA. These are not trusted roles (which are defined later in Section 5.2.1) but rather pure authorities that can be assigned to roles or offices or vendors to best fit the PKI using application. The separation of these authorities can support several purposes, including multi-party integrity (watching the watchers) and outsourcing of PKI functions.

Policy Authority: This is the entity that decides that a set of requirements for certificate issuance and use are sufficient for a given application. The Policy Authority approves the establishment of trust relationships with external PKIs that offer appropriately comparable assurance.

Trust Anchor Managers (TAMs): Authorities who manage a repository of trusted Root CA Certificates. They act on behalf of relying parties, basing their decisions on which CAs to trust on the results of compliance audits. A TAM sets requirements for inclusion of a CA's root public key in their store. These requirements are based on both security and business needs. The TAM has a duty to enforce compliance with these requirements, for example, requirements around the supply of compliance audit results, on initial acceptance of a root, and on an ongoing basis. TAMs will follow their normal practice of requiring CAs to submit an annual compliance audit report. It is our intention that the requirements in this document will be included in those compliance audit schemes. As specified in Section 5.7, the TAM will require the CA to provide notification of a compromise, and in response, the TAM will take appropriate action.

1.3.1.1 Certification Authority

The CA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to subscribers. This includes centralized, automated systems such as card management systems. The CA is responsible for issuing and managing certificates including:

- Approving the issuance of all certificates, including those issued to subordinate CAs and RAs.
- Publication of certificates
- Revocation of certificates
- Generation and destruction of CA signing keys
- Establishing and maintaining the CA system

- Establishing and maintaining the Certificate Policy (CP) & Certification Practice Statement (CPS)
- Ensuring that all aspects of the CA services, operations, and infrastructure related to certificates issued under the CP are performed in accordance with the requirements, representations, and warranties of the CP

Certification Authority (CA) Operation Staff: CA components are operated and managed by individuals holding trusted, sensitive roles. Specific responsibilities for these roles, as well as requirements for separation of duties, are described in Section 5.2.

Security Auditor: An individual (e.g. employee, contractor, consultant, 3rd party) who is responsible for auditing the security of CAs or Registration Authorities (RAs), including reviewing, maintaining, and archiving audit logs; and performing or overseeing internal audits of CAs or RAs. A single individual may audit both CAs and RAs. Security Auditor is an internal role that is designated as trusted.

1.3.1.2 Certificate Status Servers

PKIs may optionally include a service that provides status information about certificates on behalf of a CA through on-line transactions. In particular, PKIs may include Online Certificate Status Protocol (OCSP) responders to provide on-line status information. Such a service is termed a Certificate Status Server (CSS). Where the CSS is identified in certificates as an authoritative source for revocation information or issued a delegated Responder certificate, the operations of that authority are considered within the scope of this CP. A CSS shall assert all the policy OIDs for which it is authoritative. Examples include OCSP servers that are identified in the Authority Information Access (AIA) extension. OCSP servers that are locally trusted, as described in [RFC2560], are not covered by this policy.

1.3.2 Registration Authorities

The registration authorities (RAs) collect and verify each subscriber's identity and information that is to be entered into the subscriber's public key certificate. The RA performs its function in accordance with a CPS approved by the Policy Authority. The RA is responsible for:

- The registration process
- The identification and authentication process.

1.3.3 Trusted Agents

The trusted agent is a person who satisfies all the appointment requirements for an RA and who performs identity proofing as a proxy for the RA. The trusted agent records information from and verifies biometrics (e.g., fingerprints, photographs) on presented credentials for an applicant's identity on behalf of the RA. The CPS will identify the parties responsible for providing such services, and the mechanisms for determining their trustworthiness.

1.3.4 Subscribers

A subscriber is the entity whose name appears as the subject in a certificate. The subscriber asserts the use of the key and certificate in accordance with the certificate policy asserted in the certificate, and does not issue certificates. CAs are sometimes technically considered "subscribers" in a PKI. However, the term "subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

1.3.5 Relying Parties

A Relying Party is an entity that relies on the validity of the binding of the Subscriber's name to a public key. The Relying Party uses a Subscriber's certificate to verify or establish the identity and status of a system or device. A Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A Relying Party may use information in the certificate to determine the suitability of the certificate for a particular use.

1.3.6 Other Participants

The CAs and RAs operating under the CP may require the services of other security, community, and application authorities. The CPS will identify the parties responsible for providing such services, and the mechanisms used to support these services.

One such participant is the Compliance Auditor. CAs are typically required to engage organizationally-independent parties to perform compliance audits on a regular basis. To be effective, it is expected that compliance auditors will have expertise in information security, cryptography, and PKI, risk mitigation strategies, and industry best practices.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Instruction: The sensitivity of the information processed or protected using certificates issued by the CA will vary significantly. Organizations must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each organization for each application and is not controlled by the CP.

1.4.2 Prohibited Certificate Uses

Instruction: There may be instances where prohibitions are appropriate. If so, state them here.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The Policy Authority is responsible for all aspects of this CP.

1.5.2 Contact Person

Instruction: Policy Authority should identify an individual or office that can provide authoritative answers to questions that arise through the use of their CP.

1.5.3 Person Determining CPS Suitability for the Policy

The Policy Authority shall approve the CPS for each CA that issues certificates under the policy.

1.5.4 CPS Approval Procedures

CAs issuing under the policy are required to meet all facets of the policy. The Policy Authority shall work with a CA to minimize the use of waivers.

The Policy Authority shall make the determination that a CPS complies with the policy. The CA and RA must meet all requirements of an approved CPS before commencing operations. The Policy Authority will make this determination based on the nature of the system function, the type of communications, or the operating environment.

In each case, the determination of suitability shall be based on an independent compliance auditor's results and recommendations. See section 8 for further details.

1.6 Definitions and Acronyms

See Appendices A and B.

2 Publication and Repository Responsibilities

2.1 Repositories

All CAs that issue certificates under this policy are obligated to post all CA certificates issued by or to the CA and CRLs issued by the CA in a repository that is publicly accessible through all Uniform Resource Identifier (URI) references asserted in valid certificates issued by that CA. Specific example requirements are found in *Shared Service Provider Repository Service Requirements* [SSP REP]. CAs may optionally post subscriber certificates in this repository, except as noted in section 9.4.3. To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanisms to prevent unauthorized modification or deletion of information.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

The publicly accessible repository system shall be designed and implemented so as to provide <99%> availability overall and limit scheduled down-time to <0.5%> annually. Where applicable, the certificate status server (CSS) shall be designed and implemented so as to provide <99%> availability overall and limit scheduled down-time to <0.5%> annually.

2.2.2 Publication of CA Information

The CP shall be publicly available. The CPS of the CA will not be published; a CPS summary shall either be publicly available or available upon request.

2.3 Time or Frequency of Publication

An updated version of the CP will be made publicly available within <thirty> days of the incorporation of changes.

2.4 Access Controls on Repositories

The CA shall protect information not intended for public dissemination or modification. CA certificates and CRLs in the repository shall be publicly available through the Internet. Direct and/or remote access to other information in the CA repositories shall be determined by Policy Authority. The CPS shall detail what information in the repository shall be exempt from automatic availability and to whom, and under which conditions the restricted information may be made available.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The CA shall assign an X.501 Distinguished Name (DN) to each subscriber. Subscriber certificates may contain any name type appropriate to the application.

3.1.2 Need for Names to Be Meaningful

Names used in certificates must represent an unambiguous identifier for the subject. Names should be meaningful enough for a human to identify the named entity, irrespective of whether the entity is a person, machine, or process. Interpreting the name semantic may require a reference database (e.g., human resources directory or inventory catalog) external to the PKI.

Examples are:

Person Name	John Q. Public
Domain Name	publicinfo.agency.dept.gov
Machine Name	"manufacturer=DeviceCorp, model=DC-ABCD, serial=00098765"
Email Address	jqpubli@devicecorp.com
IP Address	192.168.100.75 (shall be a routable, permanent IP address)

While the issuer name in CA certificates is not generally interpreted by relying parties, this CP still requires use of meaningful names by CAs issuing under this policy. CA certificates that assert this policy shall not include a personal name, but rather shall identify the subject as a CA and include the name-space for which the CA is authoritative. For example:

cn=*OrganizationX CA-3*

The subject name in CA certificates must match the issuer name in certificates issued by the subject, as required by [RFC5280].

Instruction: If certificates are to be used in a broad context, for example on the Internet or organization-wide, specialized or difficult to interpret names should be avoided. If there is a local, name-space specific semantic to any name used, describe it here. The semantic must enable a relying party to identify a single real entity from the name.

3.1.3 Anonymity or Pseudonymity of Subscribers

The CA shall not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in X.501. Rules for interpreting e-mail addresses are specified in [RFC 2822].

Instruction: If there is a local, name-space specific name form that requires specialized interpretation, describe it here. It cannot be assumed that an arbitrary CA will be able to produce a special name form, nor that an arbitrary application will be able to interpret a special name in the desired way.

3.1.5 Uniqueness of Names

Each CA must ensure that each of its subscribers is identifiable by a unique name. Each X.500 name assigned to a subscriber by a CA (i.e., in that CA's namespace) must identify that subscriber uniquely. When other name forms are used, they too must be allocated such that each name identifies only one subscriber of that CA. Name uniqueness is not violated when multiple certificates are issued to the same entity. For certificates that assert names that do not identify individual people, the name shall be uniquely associated with a specific AOR.

The CPS shall identify the method for the assignment of unique subject names.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys, that party shall be required to prove possession of the private key, which corresponds to the public key in the certificate request. For signature keys, this may be done by the entity using its private key to sign a value supplied by the CA, which the CA will then validate. For encryption keys, the subscriber may be required to encrypt a challenge, or derive a secret shared with the CA. Other mechanisms that are at least as secure as those cited here may be added. The CA shall ensure that any mechanism or procedure used ties the private key to the identity being asserted by the subscriber.

In the case where key generation is performed under the CA or RA’s direct control, proof of possession is not required.

3.2.2 Authentication of Organization Identity

Requests for CA certificates shall include the CA name, address, and documentation of the existence of the CA. Before issuing CA certificates, an authority for the issuing CA shall verify the information, in addition to the authenticity of the requesting representative and the representative’s authorization to act in the name of the CA.

For subscriber organization certificates, the CA shall verify the existence of the organization by verifying the identity and address of the organization and that the address is the subscriber’s address of existence or operation. The CA shall verify the identity and address of the subscriber using documentation provided by, or through communication with, at least one of the following:

- Official communication with the organization;
- A third party database that is periodically updated and considered a reliable data source;
- A site visit by the CA or a third party who is acting as an agent for the CA.

The CA may use the same documentation or communication described in above to verify both the

subscriber's identity and address.

Instruction: Additional requirements that could be used for organizational identity proofing can be found at [CABF EV] Section 11.

3.2.3 Authentication of Individual Identity

Instruction: Public key certificates bind public keys to identities. However, the entity to be identified depends on the application for which the public keys are used. For instance, in a banking transaction, a certificate may name a bank account holder (i.e., a person). When two networks pass information securely, each communicating part of the network may have a certificate that identifies the device providing the security. Identifying different types of entity requires different evidence and procedures. For each type of entity engaged in the applications that this policy supports, there must be a subsection here that details the required evidence and procedure. Five are included here: human, device, application or service, role holder, and code signer. Not all PKIs will support all entity types. PKIs may support entity types not included here.

3.2.3.1 Authentication of Human Subscribers

Procedures used by organizations to issue identification to their own personnel and affiliates may be more stringent than that set forth below. When this is the case, the procedures for authentication of personnel shall apply in addition to the guidance in this section.

The RA shall ensure that the subscriber's identity information is verified. Identity shall be verified no more than <30> days before initial certificate issuance. RAs may accept authentication of a subscriber's identity attested to and documented by a trusted agent to support identity proofing of remote subscribers. Authentication by a trusted agent does not relieve the RA of its responsibility to perform steps 1), 2), the verification of identifying information (e.g., by checking official records) in step 3), and the maintenance of biometrics in step 4), below.

At a minimum, authentication procedures for human subscribers must include the following steps:

1) Verify that a request for certificate issuance to the applicant was submitted by the organization.
2) Verify Subscriber's organizational membership through use of official organization records.
3) Establish subscriber's identity by in-person proofing before the registration authority, based on the following process:
    a) The subscriber presents an official form of identification (e.g., an organization ID badge, a passport, or driver's license) as proof of identity
    b) The RA examines the presented credential that can be linked to the subscriber (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and
    c) The credential presented above shall be verified by the RA for currency and legitimacy (e.g., the organization ID is verified as valid). Typically this is accomplished by querying a database maintained by the organization that issued the credential, but other equivalent methods may be used.
4) Record and maintain a biometric of the applicant (e.g., a photograph or fingerprint) by the RA or CA. this establishes an audit trail for dispute resolution.

3.2.3.2 Authentication of Devices

Some computing and communications devices (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases, an Authorized Organizational Representative (AOR), or in certain

cases the device itself must provide identifying information for the device. The AOR/device is responsible for providing registration information which may include:

- Equipment identification (e.g., serial number)
- Equipment certificate signing request CSR
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the AOR when required.

The registration information provided by the AOR/device shall be verified. The identity of the AOR/device shall be authenticated.

3.2.3.3 Authentication of Applications or Services

Some software applications or services will be named as certificate subjects. In such cases, an Authorized Organizational Representative (AOR) must provide identifying information for the device. The AOR is responsible for providing registration information which may include:

- Unique software application or service name (e.g. DNS name)
- Software application or service certificate signing request CSR
- Software application or service authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the AOR when required.

The registration information provided by the AOR shall be verified. The identity of the AOR shall be authenticated. The CA shall validate that the AOR is the owner of the application or service by checking the appropriate and reliable 3rd party database.

Instruction: Additional requirements that could be used for application or service vetting can be found in. [CABF EV].

3.2.3.4 Authentication for Role Certificates

A role certificate shall identify a specific role on behalf of which the subscriber is authorized to act rather than the subscriber's name. A role certificate shall not be a substitute for an individual subscriber certificate. Multiple subscribers can be assigned to a role at the same time.

Subscribers issued role certificates shall protect the corresponding role credentials to the same security level as individual credentials.

The procedures for issuing role certificates shall comply with all other stipulations of this CP (e.g., subscriber identity proofing, validation of organization affiliation, key generation, private key protection, and Subscriber obligations). The AOR may act on behalf of the certificate subject for certificate management activities such as issuance, renewal, re-key, modification, and revocation.

The CA or the RA shall record the information identified in Section 3.2.3.1 for an AOR associated with the role before issuing a role certificate. The AOR shall hold an individual certificate in the subscriber's own name issued by the same CA at the same or higher assurance level as the role certificate. The CA or the RA shall validate from the AOR that the subscriber has been approved for the role certificate.

AORs shall be responsible for:

- Authorizing subscribers for a role certificate;
- Recovery of the private decryption key;
- Revocation of subscribers role certificates;
- Always maintaining a current up-to-date list of subscribers who are assigned the role; and
- Always maintaining a current up-to-date list of subscribers who have been provided the private keys for the role.

Instruction: When determining whether a role certificate is warranted, consider whether the role carries inherent authority beyond the job title. Role certificates may also be used for subscribers on temporary assignment, where the temporary assignment carries an authority not shared by the individuals in their usual occupation, for example: "Chair PKI Process Action Team".

3.2.3.5 Authentication for Code Signing Certificates

Code signing indicates to the recipient of the code that the code comes from an authorized source, and that the integrity of the source has been protected during distribution (i.e., that the code hasn't been modified). A code signing certificate identifies the person or organization authorized to make those claims to the code recipient.

The procedures for issuing code signing certificates shall comply with all other stipulations of this CP (e.g., subscriber identity proofing, validation of organization affiliation, key generation, private key protection, and Subscriber obligations). The AOR may act on behalf of the certificate subject for certificate management activities such as issuance, renewal, re-key, modification, and revocation.

The CA or the RA shall record the information identified in Section 3.2.3.1 for an AOR associated with the code signing certificate. The AOR shall hold an individual certificate in the subscriber's own name issued by the same CA at the same or higher assurance level as the role certificate. The CA or the RA shall validate from the AOR that the subscriber has been approved for the code signing certificate.

AORs shall be responsible for:

- Authorizing subscribers for a code signing certificate
- Revocation of subscriber's code signing certificates
- Always maintaining a current up-to-date list of subscribers who are assigned
- Always maintaining a current up-to-date list of subscribers who have been provided the private keys

3.2.4 Non-verified Subscriber Information

Information that is not verified shall not be included in certificates.

3.2.5 Validation of Authority

Before issuing CA certificates or signature certificates that assert organizational authority, the CA shall validate the subscriber's authority to act in the name of the organization. For role certificates that identify subjects by their organizational roles, the CA shall validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

An example of signature certificates that assert organizational authority is code signing certificates.

3.2.6 Criteria for Interoperation

Instruction: Describe in this section:

- *Whether interoperation between the CA(s) issuing certificates under this policy and other CA(s) is permitted*
- *Who makes the determination*
- *How the interoperation is accomplished (e.g., direct cross-certification bridge)- may be by reference to another document*

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

For re-key of any CA certificate issued under this certificate policy, identity may be established through use of current signature key, except that identity shall be established following the same procedures as the initial registration at least once every <number> years from the time of original registration.

For re-key of any subscriber certificate issued under this certificate policy, identity may be established through use of current signature key, except that identity shall be established following the same procedures as the initial registration at least once every <number> years from the time of original registration.

Instruction: In-person registration is considered to be more assured than one based on use of a previously certified key. Replace <NUMBER> in the previous paragraph with the number of years between mandatory in-person registrations. Once in 6 years is considered high assurance; once in 9 years is considered moderate assurance; once in 15 years is considered basic.

3.3.2 Identification and Authentication for Re-key after Revocation

In the event of certificate revocation, issuance of a new certificate shall always require that the party go through the initial registration process per Section 3.2 above.

3.4 Identification and Authentication for Revocation Request

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

The Certificate application process must provide sufficient information to:

- Establish the applicant's authorization (by the employing or sponsoring organization) to obtain a certificate. (per Section 3.2.3)
- Establish and record identity of the applicant. (per Section 3.2.3)
- Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required. (per Section 3.2.1)
- Verify any role or authorization information requested for inclusion in the certificate.

These steps may be performed in any order that is convenient for the CA and applicants that does not compromise security, but all must be completed before certificate issuance.

4.1.1 Who Can Submit a Certificate Application

A certificate application may be submitted to the CA by the Subscriber, AOR, or an RA on behalf of the Subscriber.

4.1.2 Enrollment Process and Responsibilities

All communications among PKI Authorities supporting the certificate application and issuance process shall be authenticated and protected from modification; any electronic transmission of shared secrets and personally identifiable information shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used. Out-of-band communications shall protect the confidentiality and integrity of the data.

Subscribers are responsible for providing accurate information on their certificate applications.

4.2 Certificate Application Processing

Information in certificate applications must be verified as accurate before certificates are issued. Procedures to verify information in certificate applications shall be specified in the CPS.

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of the subscriber must meet the requirements specified for subscriber authentication as specified in Sections 3.2 and 3.3. The components of the PKI (e.g., CA or RA) that are responsible for authenticating the subscriber's identity in each case must be identified in the CPS.

4.2.2 Approval or Rejection of Certificate Applications

Any certificate application that is received by a CA under this policy, for which the identity and authorization of the applicant has been validated, will be duly processed. However, the CA must reject any application for which such validation cannot be completed, or when the CA has cause to lack confidence in the application or certification process.

Instruction: This text presents a permissive approach to certificate issuance. For high-risk applications, a more restrictive approach may be desired. In some organizations, there may be a policy authority to whom to refer questionable cases.

4.2.3 Time to Process Certificate Applications

Certificate applications must be processed and a certificate issued within <time> of identity verification.

Instruction: The time it takes to process a certification request can vary greatly, depending on verification mechanisms. Device certificates might be issued instantly, while person certificates may be delayed by employee database look-ups. Replace <time> with a reasonable period for your purpose.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Upon receiving the request, the CAs/RAs will:

- Verify the identity of the requester as specified in Section 3.2.
- Verify the authority of the requester and the integrity of the information in the certificate request as specified in Section 4.1.
- Build and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate).
- Make the certificate available to the subscriber after confirming that the subscriber has formally acknowledged their obligations as described in Section 9.6.3.

The certificate request may already contain a certificate built by either the RA or the subscriber. This certificate will not be signed until all verifications and modifications, if any, have been completed to the CA's satisfaction.

All authorization and other attribute information received from a prospective subscriber shall be verified before inclusion in a certificate. The responsibility for verifying prospective subscriber data shall be described in a CA's CPS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

CAs operating under this policy shall inform the subscriber (or other certificate subject) of the creation of a certificate and make the certificate available to the subscriber. For device certificates, the CA shall issue the certificate according to the certificate requesting protocol used by the device (this may be automated) and, if the protocol does not provide inherent notification, also notify the authorized organizational representative of the issuance (this may be in batch).

4.4 Certificate Acceptance

Before a subscriber can make effective use of its private key, the CA shall explain to the subscriber its responsibilities and obtain the subscriber's acknowledgement, as defined in Section 9.6.3.

4.4.1 Conduct Constituting Certificate Acceptance

Failure to object to the certificate or its contents shall constitute acceptance of the certificate.

Instruction: This text is a generic acceptance test; it can be made stronger by tying the acceptance to the acknowledgement of the user agreement if such acknowledgement is obtained in real-time.

4.4.2 Publication of the Certificate by the CA

As specified in Section 2.1, all CA certificates shall be published in repositories.

This policy makes no stipulation regarding publication of subscriber certificates, except as noted in Section 9.4.3.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The Policy Authority must be notified whenever a CA operating under this policy issues a CA certificate.

Instruction: It is important for an organization that has established a certification policy to know when new sources of certificates that assert that policy come into being; this helps prevent rogue offerings.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The intended scope of usage for a private key is specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

4.5.2 Relying Party Public key and Certificate Usage

Certificates may specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. All CAs operating under this policy shall issue CRLs specifying the current status of all unexpired certificates except for OCSP responder certificates. It is recommended that relying parties process and comply with this information whenever using certificates in a transaction.

4.6 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been revoked or compromised, and the Subscriber name and attributes are unchanged. In addition, the validity period of the certificate must not exceed the remaining lifetime of the private key, as specified in Section 5.6. The identity proofing requirements listed in Section 3.3.1 shall also be met.

CA Certificates and OCSP responder certificates may be renewed so long as the aggregated lifetime of the public key does not exceed the certificate lifetime specified in Section 6.3.2.

The CA may renew certificates during recovery from key compromise without subject request or approval as long as the CA is confident of the accuracy of information to be included in the certificates.

4.6.2 Who May Request Renewal

For all CAs and OCSP responders operating under this policy, the corresponding operating authority may request renewal of its own certificate.

4.6.3 Processing Certificate Renewal Requests

Digital signatures on subscriber renewal requests shall be validated before electronic renewal requests are processed. Alternatively, subscriber renewal requests may be processed using the same process used for initial certificate issuance.

Instruction: Trust in the public key shall be established using certification path validation rules described in [RFC 5280], including validation of revocation status of each certificate in the path using current, valid revocation information (e.g, using a CRL whose nextUpdate field is later than the current, verification time).

4.6.4 Notification of New Certificate Issuance to Subscriber

The CA shall inform the subscriber of the renewal of his or her certificate and the contents of the certificate.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Failure to object to the renewal of the certificate or its contents constitutes acceptance of the certificate.

4.6.6 Publication of the Renewal Certificate by the CA

As specified in Section 2.1, all CA certificates shall be published in repositories.

This policy makes no stipulation regarding publication of subscriber certificates, except as noted in Section 9.4.3.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 Certificate Re-key

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. Re-key of a certificate does not require a change to the *subjectName* and does not violate the requirement for name uniqueness. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

Subscribers shall identify themselves for the purpose of re-keying as required in section 3.3.

4.7.1 Circumstance for Certificate Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a subscriber periodically obtain new keys. (Section 6.3.2 establishes usage periods for private keys for both CAs and subscribers.) Examples of circumstances requiring certificate re-key

include: expiration, loss or compromise, issuance of a new hardware token, and hardware token failure.

4.7.2 Who May Request Certification of a New Public Key

Requests for certification of a new public key shall be considered as follows:

- Subscribers with a currently valid certificate may request certification of a new public key.
- CAs and RAs may request certification of a new public key on behalf of a subscriber.
- For device certificates, an authorized representative of the organization that owns or controls the device may request re-key.

4.7.3 Processing Certificate Re-keying Requests

Digital signatures on subscriber re-key requests shall be validated before electronic re-key requests are processed. Alternatively, subscriber re-key requests may be processed using the same process used for initial certificate issuance.

Instruction: Trust in the public key shall be established using certification path validation rules described in [RFC 5280], including validation of revocation status of each certificate in the path using current, valid revocation information (e.g, using a CRL whose nextUpdate field is later than the current, verification time).

4.7.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.7.6 Publication of the Re-keyed Certificate by the CA

All CA certificates must be published as specified in Section 2.

This policy makes no stipulation regarding publication of subscriber certificates, except as noted in Section 9.4.3.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate Modification

Modifying a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

Instruction: Because of the requirement to validate a name change, and the sometimes complex combination of permissive and restrictive interpretation of certificate contents, it is often simpler and more secure to require re-certification than to offer certificate modification. This section should only be included if there is a well-defined reason to offer certificate modification.

4.8.1 Circumstance for Certificate Modification

A CA operating under this policy may modify a CA or OCSP responder certificate whose characteristics have changed (e.g. assert new policy OID). The new certificate may have the same or a different subject public key. If the assurance level of the new certificate is lower, older one must be revoked.

A CA may perform certificate modification for a subscriber whose characteristics have changed (e.g., name change due to marriage). The new certificate shall have a different subject public key.

4.8.2 Who May Request Certificate Modification

Requests for certification of a new public key shall be considered as follows:

- Subscribers with a currently valid certificate may request certificate modification.
- CAs and RAs may request certificate modification on behalf of a subscriber.
- For device certificates, an authorized representative of the organization that owns or controls the device may request certificate modification.

4.8.3 Processing Certificate Modification Requests

A certificate modification shall be achieved using one of the following processes:

- Initial registration process as described in Section 3.2
- Identification & Authentication for using digital signature as described in Section 4.7.3. In addition, the validation of the changed subject information shall be in accordance with the initial identity-proofing process as described in Section 3.2

Proof of all subject information changes must be provided to the RA or other designated agent and verified before the modified certificate is issued.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.8.6 Publication of the Modified Certificate by the CA

All CA certificates must be published as specified in section 2.

This policy makes no stipulation regarding publication of subscriber certificates, except as noted in section 9.4.3.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

CAs operating under this policy shall issue CRLs covering all unexpired certificates issued under this policy except for OCSP responder. Relying party client software may support on-line status checking and some support only CRLs. CAs should strongly consider offering online status checking in addition to CRLs.

CAs operating under this policy shall make public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to subscribers during certificate request or issuance, and shall be readily available to any potential relying party.

Revocation requests must be authenticated. See Section 3.4 for more details**.**

Certificate suspension for CA certificates is not allowed by this policy. However, the use of certificate suspension for end entity certificates is allowed.

4.9.1 Circumstances for Revocation

A certificate shall be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- Identifying information or affiliation components of any names in the certificate becomes invalid.
- Privilege attributes asserted in the subscriber's certificate are reduced.
- The subscriber can be shown to have violated the stipulations of its subscriber agreement.
- There is reason to believe the private key has been compromised.
- The subscriber or other authorized party (as defined in the CPS) asks for his/her certificate to be revoked.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

4.9.2 Who Can Request Revocation

Within the PKI, a CA may summarily revoke certificates within its domain. A written notice and brief explanation for the revocation shall subsequently be provided to the subscriber. The RA can request the revocation of a subscriber's certificate on behalf of any authorized party as specified in the CPS. A subscriber may request that its own certificate be revoked. The AOR of the organization that owns or controls a device can request the revocation of the device's certificate. Other authorized individuals of the organization may request revocation as described in the CPS.

4.9.3 Procedure for Revocation Request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The steps involved in the process of requesting a certification revocation are detailed in the CPS.

Where subscribers use hardware tokens, revocation is optional if all the following conditions are met:

- the revocation request was not for key compromise
- the hardware token does not permit the user to export private keys
- the subscriber surrendered the token to the PKI
- the token was zeroized or destroyed promptly upon surrender
- The token has been protected from malicious use between surrender and zeroization or destruction.

In all other cases, revocation of the certificates is mandatory.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this policy.

4.9.5 Time within which CA must Process the Revocation Request

CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published, excepting those requests received within <two hours> of CRL issuance.

4.9.6 Revocation Checking Requirements for Relying Parties

No stipulation.

4.9.7 CRL Issuance Frequency

CRLs shall be issued periodically per the CPS, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below.

Certificate status information shall be published no later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote (laptop) operation.

CAs that issue certificates to subscribers or operate on-line must issue CRLs at least once every <18> hours, and the *nextUpdate* time in the CRL may be no later than <48> hours after issuance time (i.e., the *thisUpdate* time).

Circumstances related to emergency CRL issuance are specified in section 4.9.12.

4.9.8 Maximum Latency for CRLs

CRLs shall be published within <4> hours of generation. Furthermore, each CRL shall be published no later than the time specified in the *nextUpdate* field of the previously issued CRL for same scope.

Instruction: The time between CRL generation and publication must be minimized to be of use to Relying Parties. A reasonable latency for the preceding paragraph is 4 hours; much shorter latency should be routinely achievable in practice.

4.9.9 On-line Revocation/Status Checking Availability

Where on-line status checking is supported, status information must be updated and available to relying parties within <4> hours of CRL publication.

Instruction: For OCSP responses to be credible, the time it takes from CRL publication to OSCP availablity should be as short as possible. A reasonable number for the number in the preceding paragraph is 4 hours. A higher assurance PKI may require faster availability; 2 hours is recommended.

4.9.10 On-line Revocation Checking Requirements

Relying party client software may optionally support on-line status checking. Client software using on-line status checking need not obtain or process CRLs.

4.9.11 Other Forms of Revocation Advertisements Available

A CA may also use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements:

- The alternative method must be described in the CA's approved CPS;
- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.
- The alternative method must meet the issuance and latency requirements for CRLs stated in Sections 4.9.7 and 4.9.8.
- Components involved in creation of revocation information including providing authentication and integrity services must meet the security requirements for CSS as stated in this CP.

4.9.12 Special Requirements Related To Key Compromise

Certificate revocation for reason of key compromise must appear in a published CRL (or OCSP response) within <6> hours of the decision to revoke.

Instruction: It's extremely important that relying parties are made aware as soon as possible when a CA knows that there is no longer a one-to-one binding between a named entity and a private key.

4.9.13 Circumstances for Suspension

Instruction: From the CA point of view, certificate suspension merely indicates some (undefined) level of doubt in the binding between subscriber name and key. From the Relying Party point of view, however, the certificate is considered to be revoked. Certificate suspension is not recommended unless there is a narrowly defined use-case and the intended Relying Party interpretation of the suspension is clearly communicated. In that case, the following subsections must be completed.

4.9.13.1 Circumstances for Suspension

For CA certificates, suspension is not permitted.

For end entity certificates, there is no stipulation.

4.9.13.2 Who Can Request Suspension

No stipulation for end entity certificates.

4.9.13.3 Procedure for Suspension Request

No stipulation for end entity certificates.

4.9.13.4 Limits on Suspension Period

No stipulation for end entity certificates.

4.9.13.5 Circumstances for Restoration

No stipulation for end entity certificates.

4.9.13.6 Who Can Request Restoration

No stipulation for end entity certificates.

4.9.13.7 Procedure for Restoration Request

No stipulation for end entity certificates.

4.10 Certificate Status Services

Instruction: There is no requirement to operate a certificate status service, but it is perceived as more efficient and can provide more timely information if the service obtains CRLs more frequently than client applications. If the organization decides to offer such a service, these sections must be completed to allow Relying Parties to decide what can be inferred from the status information they receive.

4.11 End Of Subscription

No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

CA private keys are never escrowed.

Subscriber key management keys may be escrowed to provide key recovery. Escrowed keys shall be protected at no less than the level of security in which they are generated, delivered, and protected by the subscriber. Under no circumstances shall a subscriber signature key be held in trust by a third party. CAs that support private key escrow for key management keys shall document their specific practices in their CPS.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

CAs that support session key encapsulation and recovery shall identify the document describing the practices in the applicable CPS. Components that support session key recovery shall meet the security requirements for the CAs as stated in this CP.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

All CA and RA equipment, including cryptographic modules, shall be protected from theft, loss, and unauthorized access at all times. Unauthorized use of CA and RA equipment is prohibited. CA equipment shall be dedicated to performing CA functions. RA equipment shall be operated to ensure that the equipment meets all physical controls at all times.

5.1.1 Site Location and Construction

The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CAs, shall be consistent with facilities used to house high-value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical Access

5.1.2.1 Physical Access for CA Equipment

Physical access to CA equipment shall be limited to CA Operations Staff and Security Auditors. The security mechanisms shall be commensurate with the level of threat in the equipment environment.

At a minimum, physical access controls for CA equipment and all copies of the CA cryptographic module shall meet the following requirements:

- Ensure that no unauthorized access to the hardware is permitted
- Be manually or electronically monitored for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically.
- Mandate at least two-person access requirements. At least one individual shall be a member of the CA Operations Staff. Technical or mechanical mechanisms (e.g., dual locks) shall be used to enforce the two-person physical access control
- Other individuals shall be escorted by two persons. This includes maintenance personnel. All individuals shall be recorded in the access log.

When not in use, removable CA cryptographic modules, removable media, and any activation information used to access or enable CA cryptographic modules or CA equipment, or paper containing sensitive plain-text information shall be placed in locked containers sufficient for housing equipment and information commensurate with the sensitivity, or value of the information being protected by the certificates issued by the CA. Access to the contents of the locked containers shall be restricted to individuals holding CA trusted roles as defined in Section 5.2.1, utilizing two-person access controls, and two-person integrity while the container is unlocked.

CA cryptographic modules held within the work area for intermittent use throughout the day may be kept under one lock, as long as they are stored in an area where there are at least two persons physically present at all times. Knowledge of the combination or access to the key used to secure the lock shall be restricted to authorized individuals only. When in active use, the cryptographic module shall be locked into the system or container (rack, reader, server, etc.) using a physical lock under the control of the CA Operations Staff to prevent unauthorized removal.

Any activation information used to access or enable the cryptographic modules or CA equipment shall be stored separately from the associated modules and equipment. Such information shall either be memorized or recorded and stored in a manner commensurate with the security afforded the associated cryptographic module or equipment.

A security check of the room/rack housing CA equipment shall occur prior to leaving the room/rack unattended by the CA Operations Staff. The check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when "open", and secured when "closed")
- Any security containers are properly secured
- Physical security systems (e.g., door locks, vent covers) are functioning properly
- The area is secured against unauthorized access

If unattended, the facility housing CA equipment shall be protected by an intrusion detection system (IDS).

If a facility is not continuously attended and does not include an IDS, a check shall be made at least once every <24> hours to ensure that no attempts to defeat the physical security mechanisms have been made. A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons are responsible, a log identifying the person performing a check at each instance shall be maintained. The last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 Physical Access for RA Equipment

RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. RAs shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module or physical token is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

Any activation information used to access or enable the RA equipment shall be stored separately from the associated modules and equipment. Such information shall either be memorized or recorded and stored in a manner commensurate with the security afforded the associated cryptographic module or equipment.

5.1.2.3 Physical Access for CSS Equipment

Physical access control requirements for CSS equipment (if implemented), shall meet the CA physical access requirements specified in Section 5.1.2.1.

5.1.3 Power and Air Conditioning

The CA shall have backup power capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown. The repositories (containing CA certificates and CRLs) shall be provided with uninterrupted power sufficient for a minimum of <6 hours> operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4 Water Exposures

CA equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or

elevated floors).

Potential water damage from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention and Protection

No stipulation.

5.1.6 Media Storage

Media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic) and unauthorized physical access. Media not required for daily operation or not required by policy to remain with the CA or RA that contains security audit, archive, or backup information shall be stored securely in a location separate from the CA or RA equipment.

Media containing private key material shall be handled, packaged, and stored in a manner compliant with the requirements for the sensitivity level of the information it protects or provides access. Storage protection of CA and RA private key material shall be consistent with stipulations in Section 5.1.2.

5.1.7 Waste Disposal

CA and RA Operations Staff shall remove and destroy normal office waste in accordance with local policy. Media used to collect or transmit privacy information shall be destroyed, such that the information is unrecoverable, prior to disposal. Sensitive media and paper shall be destroyed in accordance with the applicable policy for destruction of such material.

Destruction of media and documentation containing sensitive information such as private key material shall comply with stipulations in [SP 800-88].

5.1.8 Off-Site Backup

A system backup shall be made when a CA system is activated. If the CA system is operational for more than a week, backups shall be made at least once per week. Backups shall be stored offsite. Only the latest backup needs to be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA system.

The data backup media shall be stored in a facility approved for storage of information of the same value of the information that will be protected by the certificates and associated private keys issued or managed using the equipment with a minimum requirement of transferring, handling, packaging, and storage of the information in a manner compliant with requirements for sensitive material identified in Section 6.2.4.1.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. It is essential that the people selected to fill these roles shall be held accountable to perform designated actions correctly or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust in the CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first approach is to

minimize the number of trusted roles and ensure that the people filling those roles are trustworthy and properly trained. The second is to enforce the concept of least privilege and distribute the functions of the roles among several people, so that any malicious activity requires collusion.

Trusted role operations include:

- The validation, authentication, and handling of information in Certificate Applications
- The acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrollment information
- The issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository
- Access to safe combinations and/or keys to security containers that contain materials supporting production services
- Access to hardware security modules (HSMs), their associated keying material, and the secret share splits of the PINS that protect access to the HSMs
- Providing enterprise customer support
- Access to any source code for the digital certificate applications or systems.
- Access to restricted portions of the certificate repository
- The ability to grant physical and/or logical access to the CA equipment
- The ability to administer the background investigation policy processes

The only mandatory trusted roles defined by this policy are the Administrators, CA Operations Staff, the RA Operations Staff and Security Auditors. Multiple people may hold the same trusted role, with collective privileges sufficient to fill the role. Other trusted roles may be defined in other documents, which describe or impose requirements on the CA operation.

The CA shall maintain lists, including names, organizations, contact information, and organizational affiliation for those who act in Administrator, CA Operations Staff, RAs, and Security Auditor trusted roles, and shall make them available during compliance audits. The RA shall maintain lists, including names, organizations, and contact information of those who act in RA Operations Staff, RA Administrators, and RA Security Auditor roles for that RA.

5.2.1.1 Administrator

The administrator role shall be responsible for:

- Installation, configuration, and maintenance of the CA and CSS (where applicable)
- Establishing and maintaining CA and CSS system accounts
- Configuring certificate profiles or templates
- Configuring CA, RA, and CSS audit parameters
- Configuring CSS response profiles
- Generating and backing up CA and CSS keys
- Controlling and managing CA cryptographic modules
- System backups and recovery
- Changing recording media

Administrators do not issue certificates to subscribers.

5.2.1.2 CA Operation Staff

The CA Operation Staff role shall be responsible for issuing certificates, that is:

- Registering new subscribers and requesting the issuance of certificates
- Verifying the identity of subscribers and accuracy of information included in certificates
- Approving and executing the issuance of certificates
- Requesting, approving and executing the revocation of certificates
- Approving infrastructure certificates issued to support the operations of the CA
- Approving revocation of certificates issued to CAs or to support the operations of the CA
- Approving certificates issued to RAs
- Authorizing RAs
- Approving revocation of certificates issued to RAs
- Providing Certificate revocation and suspension status information as part of a CSS (if implemented)
- Posting Certificates and CRLs

5.2.1.3 Auditor

Security Auditors are responsible for auditing CAs and RAs. This sensitive role cannot be combined with any other sensitive role, e.g. the Security Auditor cannot also be part of the CA Operations Staff. Security Auditors are responsible for reviewing, maintaining, and archiving audit logs, and for performing or overseeing internal audits (independent of formal compliance audits) to ensure that CAs and RAs are operating in accordance with the associated CPSs.

1.1.1.1 RA Staff

RA Staff are the individuals holding trusted roles that operate and manage RA components. RA Staff is responsible for the following:

- Installation, configuration, and maintenance of the RA
- Establishing and maintaining RA operating system and application accounts
- Routine operation of the RA equipment such as system backup and recovery or changing recording media
- Registering new Subscriber and requesting the issuance of certificates
- Verifying the identity of Subscribers
- Verifying the accuracy of information included in certificates
- Approving and executing the issuance of certificates
- Requesting, approving, and executing the suspension, restoration, and revocation of certificates

5.2.2 Number of Persons Required per Task

Where multi-party control is required, all participants shall hold a trusted role. Multi-party control shall not be achieved using personnel that serve in a Security Auditor role with the exception of audit functions. The following tasks shall require two or more persons:

- Generation, activation, and backup of CA keys
- Performance of CA administration or maintenance tasks
- Archiving or deleting CA audit logs. At least one of the participants shall serve in a Security Auditor role.
- Physical access to CA equipment

- Access to any copy of the CA cryptographic module
- Processing of third party key recovery requests

5.2.3 Identification and Authentication for Each Role

Individuals holding trusted roles shall identify themselves and be authenticated by the CA and RA before being permitted to perform any actions set forth above for that role or identity. CA Operations Staff and RA Staff shall authenticate using a credential that is distinct from any credential they use to perform non-trusted role functions. This credential shall be generated and stored in a system that is protected to the same level as the CA system.

CA and RA equipment shall require, at a minimum, strong authenticated access control for remote access using multi-factor authentication. Examples of multi factor authentication include use of a password or PIN along with a time-based token, digital certificate on a hardware token or other device that enforce a policy of what a user has and what a user knows.

CA and RA equipment shall require, at a minimum, authenticated access control (e.g., strong passwords) for local multi-party access.

Individuals holding trusted roles shall be appointed to the trusted role by an appropriate approving authority. The approval shall be recorded in a secure and auditable fashion. Individuals holding trusted roles shall accept the responsibilities of the trusted role, and this acceptance shall be recorded in a secure and auditable fashion.

Identity proofing of the RA shall be performed by a member of the CA Operations Staff.

Users shall authenticate themselves to all aspects of the network (servers, operating systems, applications, databases, processes, and so on) before they can access that resource.

5.2.3.1 Authentication: Passwords and Accounts

When the authentication mechanism uses operator selectable passwords, strong passwords shall be employed, as defined in <organization password policy>. Passwords for CA authentication shall be different from non-CA systems.

Instruction: Use of passwords for authentication is discouraged because they can be difficult to remember and easy to guess. However, they remain the most common form of system access authentication. Organizations generally have a policy regarding passwords and their management; if so, this policy should be referenced. Features of a good password policy generally include:

- at least 12 characters long
- a mix of uppercase and lowercase characters, numbers, and symbols
- no consecutive repeating characters (for example, RR or 55)
- not based on username, personal information, or dictionary words
- dissimilar to previous passwords
- regularly changed (for instance, every 90 days)

The CA shall have the minimum number of accounts that are necessary to its operation. Account access shall be locked after <number, usually 3 to 5> unsuccessful login attempts. Restoration of access shall be performed by a different person who holds a trusted role.

5.2.4 Roles Requiring Separation of Duties

Individuals serving as Security Auditors shall not perform or hold any other trusted role.

An individual that holds any CA Operations Staff role shall not be an RA except that CA Operations Staff may perform RA functions when issuing CA Certificates or issuing certificates to RA.

Under no circumstances shall a CA provider be audited for compliance by any subsidiary, parent, or sibling company of its corporate holdings.

Only an individual serving in a Security Auditor role may perform internal auditing functions, with the exception of those security audit functions (e.g., configuring, archiving, deleting) that require multi-person control.

An individual that performs any trusted role shall only have one identity when accessing CA equipment.

5.3 Personnel Controls

Personnel Security plays a critical role in the CA facility's overall security system. Personnel Security shall be designed to prevent both unauthorized access to the CA facility and CA systems and compromise of sensitive CA operations by CA personnel.

Inadequate personnel security procedures or negligent enforcement of personnel security policies can pose potentially devastating threats to security. These threats can include unauthorized access, data loss and corruption, denial of service, and even facility sabotage and terrorism. Such events can erode or destroy customer confidence in the CA.

5.3.1 Qualifications, Experience, and Clearance Requirements

Personnel seeking to become Trusted Persons shall present proof of the requisite background, qualifications and experience needed to perform their prospective job responsibilities competently and satisfactorily.

Individuals appointed to any trusted role shall meet the following:

- Be employees of or contractor/vendor of the CA and bound by terms of employment or contract
- Be appointed in writing
- Have successfully completed an appropriate training program
- Have demonstrated the ability to perform their duties
- Have no other duties that would interfere or conflict with their responsibilities as defined in Section 5.2.1
- Have not been previously relieved of trusted role duties for reasons of negligence or non-performance of duties

5.3.2 Background Check Procedures

Persons fulfilling Trusted Roles shall pass a comprehensive background check. CAs shall have a process in place to ensure employees undergo background checks at least every <5> years.

Prior to commencement of employment in a Trusted Role, the CA shall conduct background checks (in accordance with local privacy laws) which include the following:

- Confirmation of previous employment
- Check of professional reference
- Confirmation of the highest or most relevant educational degree obtained
- Search of criminal records (local, state or provincial, and national)
- Check of credit/financial records
- Search of driver's license records
- Identification verification via National Identity Check (e.g., Social Security Administration records), as applicable

Factors revealed in a background check that should be considered grounds for rejecting candidates for Trusted Roles or for taking action against an existing Trusted Person generally include (but are not limited to) the following:

- Misrepresentations made by the candidate or Trusted Person
- Highly unfavorable or unreliable professional references
- Certain criminal convictions
- Indications of a lack of financial or personal responsibility

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the CA, CSS or RA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA/CSS/RA security principles and mechanisms
- All PKI software versions in use on the CA/CSS/RA system
- All PKI duties they are expected to perform
- Disaster recovery and business continuity procedures
- Stipulations of this policy

5.3.4 Retraining Frequency and Requirements

All individuals responsible for PKI Trusted Roles shall be made aware of changes in the CA, CSS, RA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Appropriate administrative and disciplinary actions as documented in organization policy shall be taken against personnel who perform unauthorized actions (i.e., not permitted by this CPS or other policies) involving the CA's systems, the certificate status verification systems, and the repository. Disciplinary actions may include measures up to and including termination and shall be commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

Contractor personnel filling trusted roles shall be subject to all requirements stipulated in this document. Independent contractors and consultants who have not completed or passed the background check procedures specified above shall be permitted access to the CA's secure facilities only to the extent they are escorted and directly supervised by a person holding trusted role at all times.

5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role.

5.4 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the CAs, CSS, and RAs. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

5.4.1 Types of Events Recorded

All security auditing capabilities of CA, CSS, and RA operating system and applications shall be enabled during installation. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event;
- The date and time the event occurred;
- Success or failure where appropriate, and
- The identity of the entity and/or operator that caused the event.

A message from any source requesting an action by the CA, CSS or RA is an auditable event; the corresponding audit record must also include message date and time, source, destination, and contents.

The CA, CSS and RA shall record the events identified in the list below. Where these events cannot be electronically logged, the CA/CSS/RA shall supplement electronic audit logs with physical logs as necessary.

- SECURITY AUDIT:
  - Any changes to the Audit parameters, e.g., audit frequency, type of event audited
  - Any attempt to delete or modify the Audit logs
  - Obtaining a third-party time-stamp
- IDENTIFICATION AND AUTHENTICATION:
  - Successful and unsuccessful attempts to assume a role
  - The value of maximum authentication attempts is changed
  - Maximum unsuccessful authentication attempts occur during user login
  - An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
  - An Administrator changes the type of authenticator, e.g., from password to biometrics
  - Attempts to set passwords
  - Attempts to modify passwords
  - Logon attempts to CA, CSS or RA applications

    - Escalation of privilege
- LOCAL DATA ENTRY:
    - All security-relevant data that is entered in the system
- REMOTE DATA ENTRY:
    - All security-relevant messages that are received by the system
- DATA EXPORT AND OUTPUT:
    - All successful and unsuccessful requests for confidential and security-relevant information
- KEY GENERATION:
    - Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)
- PRIVATE KEY LOAD AND STORAGE:
    - The loading of Component private keys
    - All access to certificate subject private keys retained within the CA for key recovery purposes
- TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE:
    - All changes to the trusted public keys, including additions and deletions
- SECRET KEY STORAGE:
    - The manual entry of secret keys used for authentication
- PRIVATE AND SECRET KEY EXPORT:
    - The export of private and secret keys (keys used for a single session or message are excluded)
- CERTIFICATE REGISTRATION:
    - All certificate requests
- CERTIFICATE REVOCATION:
    - All certificate revocation requests
- TOKEN MANAGEMENT
    - Loading tokens with certificates
    - Shipment of tokens
    - Zeroizing tokens
- CERTIFICATE STATUS CHANGE APPROVAL:
    - The approval or rejection of a certificate status change request
- CA/CSS/RA CONFIGURATION:
    - Installation of the operating system
    - Installation of the CA, CSS or RA
    - Installing hardware cryptographic modules
    - Removing hardware cryptographic modules
    - Re-key of the CA, CSS or RA
    - Destruction of cryptographic modules
    - System startup
    - Any security-relevant changes to the configuration of the CA, CSS or RA
- ACCOUNT ADMINISTRATION:
    - Roles and users are added or deleted
    - The access control privileges of a user account or a role are modified
    - Appointment of an individual to a trusted role
    - Designation of personnel for multi-party control
- CERTIFICATE PROFILE MANAGEMENT:
    - All changes to the certificate profile
- REVOCATION PROFILE MANAGEMENT:
    - All changes to the revocation profile

- CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT:
  - All changes to the certificate revocation list profile
- MISCELLANEOUS:
  - Receipt of hardware / software
  - Backing up CA, CSS or RA internal database
  - Restoring CA, CSS or RA internal database
  - File manipulation (e.g., creation, renaming, moving)
  - Posting of any material to a repository
  - Access to CA, CSS or RA internal database
  - All certificate compromise notification requests
  - Configuration changes to the CA, CSS or RA server involving:
  - Hardware
  - Software
  - Operating system
  - Patches
  - Security profiles
- PHYSICAL ACCESS / SITE SECURITY:
  - Personnel access to room housing CA, CSS, or RA
  - Access to the CA, CSS, or RA server
  - Known or suspected violations of physical security
  - Any removal or addition of equipment to the CA/CSS/RA enclosure. (Equipment sign-out and return)
- ANOMALIES:
  - Software error conditions
  - Software check integrity failures
  - Receipt of improper messages
  - Misrouted messages
  - Network attacks (suspected or confirmed)
  - Equipment failure
  - Electrical power outages
  - Uninterruptible power supply (UPS) failure
  - Obvious and significant network service or access failures
  - Violations of certificate policy
  - Violations of certification practice statement
  - Resetting operating system clock

5.4.2 Frequency of Processing Log

The audit log shall be reviewed at least once every <number> days. All significant events shall be explained in an audit log summary. Actions taken as a result of these reviews shall be documented.

Such reviews involve verifying that the log has not been tampered with and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. A statistically significant portion of the security audit data generated by the CA, CSS and RA since the last review shall be examined. This amount will be described in the CPS.

Real-time automated analysis tools should be used. All alerts generated by such a systems shall be analyzed.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained on-site for at least <number> days in addition to being archived as described in section 5.5. The individual who removes audit logs from the CA system shall be an official different from the individuals who, in combination, command the CA signature key. For the CSS and RA, a System Administrator other than the CSS operator or RA shall be responsible for managing the audit log.

5.4.4 Protection of Audit Log

The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing.

Electronic logs shall be protected to prevent alteration and detect tampering. Examples include digitally signing audit records or the use of a data diode to transfer logs to a separate system to prevent modification after the log is written to media.

Physical logbooks shall implement controls to allow for the detection of the removal of pages or deletion of entries.

Security audit data shall be moved to a safe, secure storage location separate from the location where the data was generated.

CA/CSS/RA system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data. Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access).

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up at least every <number> days. A copy of the audit log shall be sent off-site every <number> days.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system may or may not be external to the CA/CSS/RA system. Automated audit processes shall be invoked at system or application startup, and cease only at system or application shutdown. Audit collection systems shall be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files). Should it become apparent that an automated audit system has failed; CA/CSS/RA operations shall be suspended until the security audit capability can be restored.

5.4.7 Notification to Event-Causing Subject

There is no requirement to notify a subject that an event was audited. Real-time alerts are neither required nor prohibited by this policy.

5.4.8 Vulnerability Assessments

The CA shall perform routine self-assessments of security controls.

5.5 Records Archival

5.5.1 Types of Events Archived

CA/CSS/RA archive records shall be sufficiently detailed to determine the proper operation of the CA/CSS/RA and the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data shall be recorded for archive:

- CA/CSS/RA accreditation (if applicable)
- Certificate policy
- Certification practice statement
- Contractual obligations
- Other agreements concerning operations of the CA/CSS/RA
- System and equipment configuration
- Subscriber identity authentication data as per section 3.2.3
- Documentation of receipt and acceptance of certificates (if applicable)
- Subscriber agreements
- Documentation of receipt of tokens
- All CRLs issued and/or published
- All Audit logs
- Other data or applications to verify archive contents
- Compliance Auditor reports
- Any changes to the Audit parameters, e.g. audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- All access to certificate subject private keys retained within the CA for key recovery purposes
- All changes to the trusted public keys, including additions and deletions
- Remedial action taken as a result of violations of physical security
- Violations of Certificate Policy
- Violations of Certification Practice Statement

Many other relevant CA operations events are recorded in the audit logs, and archived with those logs.

5.5.2 Retention Period for Archive

Archive records must be kept for a minimum of <10-20> years and <6> months without any loss of data.

5.5.3 Protection of Archive

No unauthorized user shall be permitted to write to, modify, or delete the archive. For the CA and CSS, the authorized individuals are Security Auditors. For the RA, authorized individuals are someone other than the RA.

For the CA/CSS/RA, archived records may be moved to another medium. The contents of the archive shall not be released except in accordance with sections 9.3and 9.4. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents.

Archive media shall be stored in a safe, secure storage facility separate from the CA/CSS/RA with physical and procedural security controls equivalent to or better than those of the CA/CSS/RA. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the

archived data to new media shall be defined by the archive site.

5.5.4 Archive Backup Procedures

The CPS or a referenced document shall describe how archive records are backed up, and how the archive backups are managed.

5.5.5 Requirements for Time-Stamping of Records

CA/CSS/RA archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

5.5.6 Archive Collection System (Internal or External)

Archive data may be collected in any expedient manner.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures, detailing how to create, verify, package, transmit, and store the CA archive information, shall be published in the CPS.

5.6 Key Changeover

To minimize risk from compromise of a CA's private signing key, that key may be changed often. From that time on, only the new key will be used to sign CA and subscriber certificates. If the old private key is used to sign OCSP responder certificates or CRLs that cover certificates signed with that key, the old key must be retained and protected.

The CA's signing key shall have a validity period as described in section 6.3.2.

When a CA updates its private signature key and thus generates a new public key, the CA shall notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed. When a CA that distributes self-signed certificates updates its private signature key, the CA shall generate key rollover certificates, where the new public key is signed by the old private key, and vice versa. This permits acceptance of newly issued certificates and CRLs without distribution of the new self-signed certificate to current users. Key rollover certificates are optional for CAs that do not distribute self-signed certificates.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

CA organizations shall have an Incident Response Plan as specified in [SP 800-61] and a Disaster Recovery Plan.

If compromise of a CA is suspected, an independent, third-party investigation shall be performed in order to determine the nature and the degree of damage. Certificates issued off that CA shall be stopped immediately upon detection of a compromise. If a CA private signing key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA private key needs to be declared compromised. The independent, third-party investigating party shall make the determination that a CA private key has been compromised.

In case of a CSS key compromise, all certificates issued to the CSS shall be revoked and the revocation information shall be published immediately in the most expeditious manner. Subsequently, the CSS shall be re-keyed.

The vendor shall notify the trust anchor managers in the case of a root CA or notify the superior CA in the case of a subordinate CA if any of the following occur:

- Suspected or detected compromise of any CA system or subsystem
- Physical or electronic penetration of any CA system or subsystem
- Successful denial of service attacks on any CA system or subsystem
- Any incident preventing a CA from issuing and publishing a CRL or OCSP prior to the time indicated in the *nextUpdate* field in the currently published CRL or OCSP suspected or detected compromise of a certificate status server (CSS) if
    - the CSS certificate has a lifetime of more than <72> hours; and
    - the CSS certificate cannot be revoked (e.g., an OCSP responder certificate with the *id-pkix-ocsp-nocheck* extension)

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

When computing resources, software, and/or data are corrupted, CAs operating under this policy shall respond as follows:

- Notify trust anchor managers or the superior CA as soon as possible.
- Ensure that the system's integrity has been restored prior to returning to operation and determine the extent of loss of data since the last point of backup.
- If the CA signing keys are not destroyed, the integrity of the system has been restored, and the risk is deemed negligible, reestablish CA operations, giving priority to the ability to generate certificate status information within the CRL issuance schedule.
- If the CA signing keys are destroyed, the integrity of the system cannot be restored, or the risk is deemed substantial, reestablish CA operations as quickly as possible, giving priority to the generation of a new CA signing key pair.

5.7.3 Entity (CA) Private Key Compromise Procedures

5.7.3.1 Root CA Compromise Procedures

In the case of the Root CA compromise, the vendor shall notify the trust anchor managers and relying parties via public announcement, and any cross-certified PKIs, of the Root CA compromise so that they can revoke any cross certificates issued to the Root CA or any Subordinate CAs and notify all Subscribers and Relying Parties to remove the trusted self-signed certificate from their trust stores. Notification shall be made in an authenticated and trusted manner. Initiation of notification to the trust anchor managers and any cross-certified PKIs shall be made at the earliest feasible time and shall not exceed <24> hours beyond determination of compromise or loss unless otherwise required by law enforcement. Initiation of notification to relying parties and subscribers may be made after mediations are in place to ensure continued operation of applications and services. If the cause of the compromise can be adequately addressed, and it is determined that the PKI can be securely re-established, the vendors shall then generate a new Root CA certificate, solicit requests and issue new Subordinate CA certificates, securely distribute the new Root CA certificate, and re-establish any cross certificates.

5.7.3.2 Intermediate or Subordinate CA Compromise Procedures

In the event of an Intermediate or Subordinate CA key compromise, the CA vendor shall notify the trust anchor managers and Superior CA. The superior CA shall revoke that CA's certificate, and the revocation information shall be published immediately in the most expedient, authenticated, and trusted manner but within <18> hours after the notification. The Compromised CA vendor shall also investigate and report to the trust anchor mangers and Superior CA what caused the compromise or loss, and what measures have been taken to preclude recurrence. If the cause of the compromise can be adequately addressed and it is determined that the CA can be securely re-established, then, the CA shall be re-established. Upon re-establishment of the CA, new Subscriber certificates shall be requested and issued.

For Subordinate CAs, when a Subscriber certificate is revoked because of compromise, suspected compromise, or loss of the private key, a CRL shall be published at the earliest feasible time by the supporting CA, but in no case more than 6 hours after notification.

5.7.3.3 CSS Compromise Procedures

In case of a CSS key compromise, the CA that issued the CSS a certificate shall revoke that certificate, and the revocation information shall be published immediately in the most expedient, authenticated, and trusted manner. The CSS shall subsequently be re-keyed. If the CSS is self-signed and the CSS certificate expiration is more than <7> days away, the vendor shall immediately notify the trust anchor managers, relying parties, and any cross-certified PKIs of the CSS compromise so that they can notify all Subscribers and Relying Parties to remove trust in the CSS certificate from each Relying Party application, and install the re-keyed certificate.

It is recommended that the CSS have certificates with shorter lifetimes. A shorter lifetime minimizes the time that a compromised certificate is available.

5.7.3.4 RA Compromise Procedures

In case of an RA compromise, the CA shall disable the RA. In the case that an RA's key is compromised, the CA that issued the RA certificate shall revoke it, and the revocation information shall be published within <24> hours in the most expedient, authenticated, and trusted manner. The compromise shall be investigated by the CA in order to determine the actual or potential date and scope of the RA compromise. All certificates approved by that RA since the date of actual or potential RA compromise shall be revoked. In the event that the scope is indeterminate, then the CA compromise procedures in Section 5.7.3.2 shall be followed.

5.7.4 Business Continuity Capabilities after a Disaster

CAs shall be required to maintain a Disaster Recovery Plan.

In the case of a disaster in which the CA equipment is damaged and inoperative, the CA operations shall be re-established as quickly as possible, giving priority to the ability to revoke Subscriber's certificates. If the CA cannot re-establish revocation capabilities prior to date and time specified in the *nextUpdate* field in the currently published CRL issued by the CA, then the inoperative status of the CA shall be reported to the trust anchor managers and Superior CA. The trust anchor managers and Superior CA shall decide whether to declare the CA private signing key as compromised and re-establish the CA keys and certificates, or allow additional time for reestablishment of the CA's revocation capability.

In the case of a disaster whereby a CA installation is physically damaged and all copies of the CA

signature key are destroyed as a result, the CA shall request that its certificates be revoked. The CA installation shall then be completely rebuilt by re-establishing the CA equipment, generating new private and public keys, being re-certified, and re-issuing all cross certificates. Finally, all Subscriber certificates will be re-issued. In such events, any Relying Parties who continue to use certificates signed with the destroyed private key do so at their own risk, and the risk of others to whom the data is forwarded, as no revocation information will be available (if the CRL signing key was destroyed).

5.8 CA or RA Termination

When a CA operating under this policy terminates operations before all certificates have expired, Entities will be given as much advance notice as circumstances permit.

Prior to CA termination, notice shall be provided to all cross-certified CAs requesting revocation of all certificates issued to it. In addition:

- The CA shall issue a CRL revoking all unexpired certificates prior to termination. This CRL shall be available until all certificates issued by the CA expire.
- The CA, CSS, and RA shall archive all audit logs and other records prior to termination
- The CA, CSS, and RA shall destroy all its private keys upon termination
- The CA, CSS, and RA archive records shall be transferred to an appropriate authority specified in the CPS
- If a Root CA is terminated, the Root CA shall use secure means to notify the subscribers to delete all trust anchors representing the terminated CA.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

Cryptographic keying material used by CAs to sign certificates, CRLs or status information shall be generated in [FIPS 140] Level 3 validated cryptographic modules. Multi-party control is required for CA key pair generation, as specified in section 6.2.2.

CA key pair generation must create a verifiable audit trail demonstrating that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. An independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

6.1.1.2 RA Key Pair Generation

Cryptographic keying material used by RAs to sign request and authenticate to the CA shall be generated in [FIPS 140] Level 2 validated hardware cryptographic modules.

6.1.1.3 Subscriber Key Pair Generation

Subscriber key pair generation may be performed by the subscriber, CA, or RA. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in section 6.1.2 must also be met.

[FIPS 140] validated software or hardware cryptographic modules shall be used to generate all subscriber key pairs, as well as pseudo-random numbers and parameters used in key pair generation.

Instruction: If subscriber hardware tokens are required, then signature keys must be generated on the hardware token to support source authentication.

6.1.1.4 CSS Key Pair Generation

Cryptographic keying material used by CSSes to sign status information shall be generated in [FIPS 140] Level 3 validated cryptographic modules.

6.1.2 Private Key Delivery to Subscriber

If subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

When CAs or RAs generate keys on behalf of the subscriber, then the private key must be delivered securely to the subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met:

- Anyone who generates a private signing key for a subscriber shall not retain any copy of the signing key after delivery of the private signing key to the subscriber.

- The private key(s) must be protected from activation, compromise, or modification during the delivery process.
- The subscriber shall acknowledge receipt of the private key(s).
- Delivery shall be accomplished in a way that ensures that the correct keys and activation data are provided to the correct subscribers.
    - For hardware modules, accountability for the location and state of the module must be maintained until the subscriber accepts possession of it.
    - For electronic delivery of private keys, the key material shall be encrypted using a FIPS-approved cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.

The CA must maintain a record of the subscriber acknowledgment of receipt of the key.

6.1.3 Public Key Delivery to Certificate Issuer

Where key pairs are generated by the subscriber or RA, the public key and the subscriber's identity must be delivered securely to the CA for certificate issuance. The delivery mechanism shall bind the subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate.

6.1.4 CA Public Key Delivery to Relying Parties

The public key of a root CA shall be provided to the subscribers acting as relying parties in a secure manner so that it is not vulnerable to modification or substitution. Examples of acceptable methods for delivery of the public key include:

- Secure distribution of self-signed certificates through secure out-of-band mechanisms;
- Comparison of the hash of the self-signed certificate against a hash value made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not acceptable as an authentication mechanism);

When a CA updates its signature key pair, the key rollover certificates may be signed with the CA's current private key; in this case secure distribution is not required.

6.1.5 Key Sizes

This CP requires use of RSA PKCS #1, RSASSA-PSS, DSA, or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy shall contain RSA or elliptic curve public keys.

Root CA certificates shall contain subject public keys of at least 2048 bits for RSA/DSA, at least 256 bits for elliptic curve, and be signed with the corresponding private key.

CAs that generate certificates and CRLs under this policy should use the SHA-256, or SHA-384 hash algorithm when generating digital signatures. ECDSA signatures on certificates and CRLs shall be generated using SHA-256 or SHA-384, as appropriate for the key length. CAs that issue certificates signed with SHA-256 or SHA-384 must not issue certificates signed with SHA-1.

RSA signatures on CRLs that only provide status information for certificates that were generated using SHA-1 may continue to be generated using SHA-1.

Where implemented, CSSs shall sign responses using the same signature algorithm, key size, and hash

algorithm used by the CA to sign CRLs.

6.1.6 Public Key Parameters Generation and Quality Checking

Elliptic Curve public key parameters shall always be selected from the set specified in section 7.1.3.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates shall include a critical key usage extension.

Public keys that are bound into user certificates shall be used only for signing or encrypting, but not both. User certificates that contain signature keys shall assert the *digitalSignature* bit. User certificates that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit. User certificates that contain elliptic curve public keys that are to be used for key agreement shall assert the *keyAgreement* bit.

Public keys that are bound into CA certificates shall be used only for signing certificates and status information (e.g., CRLs). CA certificates whose subject public key is to be used to verify other certificates shall assert the *keyCertSign* bit. CA certificates whose subject public key is to be used to verify CRLs shall assert the *cRLSign* bit. CA certificates whose subject public key is to be used to verify Online Certificate Status Protocol (OCSP) responses shall assert the *digitalSignature* bit.

Public keys that are bound into device, applications, and service certificates may be used for digital signature (including authentication), key management, or both. Device certificates to be used for digital signatures shall assert the *digitalSignature* bit. Device certificates that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit. Device certificates that contain elliptic curve public keys that are to be used for key agreement shall assert the *keyAgreement* bit. Device certificates to be used for both digital signatures and key management shall assert the *digitalSignature* bit and either the *keyEncipherment* (for RSA) or *keyAgreement* (for elliptic curve) bit. Device certificates shall not assert the *nonRepudiation* bit.

The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits shall not be asserted in certificates issued under this policy. In addition, *anyExtendedKeyUsage* shall not be asserted in extended key usage extensions.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

CAs shall use a [FIPS 140] Level 3 or higher validated hardware cryptographic module for signing operations. RAs shall use a [FIPS 140] Level 2 or higher validated hardware cryptographic module for signing operations.

CSSes that provide status information shall use a [FIPS 140] Level 3 or higher validated hardware cryptographic module for signing operations.

Subscribers shall use a [FIPS 140] Level 1 or higher validated cryptographic module for all cryptographic operations.

6.2.2 Private Key (N of M) Multi-Person Control

A single person shall not be permitted to activate or access any cryptographic module that contains the complete CA signing key. CA signing keys may be backed up only under two-person control. Access to CA signing keys backed up for disaster recovery shall be under at least two-person control. The names of the parties used for two-person control shall be maintained on a list that shall be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

CA private keys are never escrowed.

Subscriber key management keys may be escrowed to provide key recovery as described in section 4.12.1. If a device has a separate key management key certificate, the key management private key may be escrowed. The private key associated with a certificate that asserts a digitalSignatrue key usage shall not be escrowed.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

The CA private signature keys shall be backed up under the same multiparty control as the original signature key. At least one copy of the private signature key shall be stored off-site. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original. Backup procedures shall be included in the CA's CPS.

6.2.4.2 Backup of Human Subscriber Private Keys

Backed up human subscriber private keys shall not be stored in plaintext form outside the cryptographic module. Storage must ensure security controls consistent with the protection provided by the subscriber's cryptographic module.

6.2.4.3 Backup of CSS Private Key

CSS private keys may be backed up. If backed up, all copies shall be accounted for and protected in the same manner as the original.

6.2.4.4 Backup of Device Private Keys

Device private keys may be backed up or copied, but must be held under the control of the device's AOR. Backed up device private keys shall not be stored in plaintext form outside the cryptographic module. Backup copies shall be controlled at the same security level as the original cryptographic module.

6.2.5 Private Key Archival

CA private signature keys and subscriber private signature keys shall not be archived. CAs that retain subscriber private encryption keys for business continuity purposes shall archive such subscriber private keys in accordance with section 5.5.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA private keys may be exported from the cryptographic module only to perform CA key backup

procedures as described in Section 6.2.4.1. At no time shall the CA private key exist in plaintext outside the cryptographic module.

All other keys shall be generated by a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic module boundary.

Symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in [FIPS 140].

6.2.8 Method of Activating Private Key

The subscriber must be authenticated to the cryptographic token before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to passphrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

A device may be configured to activate its private key without requiring activation data, provided that appropriate physical and logical access controls are implemented for the device and its cryptographic token. The AOR is responsible for ensuring that the system has security controls commensurate with the level of threat in the device's environment. These controls shall protect the device's hardware, software, and the cryptographic token and its activation data from compromise.

6.2.9 Method of Deactivating Private Key

Cryptographic modules that have been activated shall not be available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure or automatically after a period of inactivity as defined in the applicable CPS. CA cryptographic modules shall be removed and stored in a secure container when not in use.

6.2.10 Method of Destroying Private Key

Individuals in trusted roles shall destroy CA, RA, and CSS (e.g., OCSP server) private signature keys when they are no longer needed. Subscribers shall either surrender their cryptographic module to CA/RA personnel for destruction or destroy their private signature keys, when they are no longer needed or when the certificates to which they correspond expire or are revoked. Physical destruction of hardware is not required.

To ensure future access to encrypted data, subscriber private key management keys may be secured in long-term backups or archived.

6.2.11 Cryptographic Module Rating

See section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2 Certificate Operational Periods and Key Usage Periods

Instruction: Special consideration must be given when a CA issues certificates for multiple applications that have different validity periods, for instance S/MIME certificates and code-signing certificates. Each type of subscriber will have a different date past which it will not be able to obtain a certificate for the full validity period. Whether that timing is managed by the issuing CA or the subscriber is implementation dependent.

Instruction: Validation of a subscriber certificate requires the valid issuing CA's certificate. A subscriber certificate that is issued just before the expiration of the issuing CA's certificate will only validate during the short time that remains in the CA's certificate validity period, regardless of the validity period asserted in the subscriber certificate. Therefore, a rule-of-thumb is to stop issuing subscriber certificates with a CA private key one subscriber certificate validity period before the expiration of the issuing CA's certificate. Another way to think about this is that no subscriber certificate shall have an expiration date beyond the expiration date in the issuing CA's certificate.

The usage period for the Root CA key pair is a maximum of <number> years.

For all other CAs operating under this policy, the usage period for a CA key pair is a maximum of <number> years. The CA private key may be used to sign certificates for at most <number> years, but may be used to sign CRLs and OCSP responder certificates for the entire usage period. All certificates signed by a specific CA key pair must expire before the end of that key pair's usage period.

Instruction: Subscribers should be aware of applications that have long term uses. For instance, data that is stored with its original encryption or documents that are stored with their original digital signatures may require special processing because all of the keys and certificates originally used will have expired or exceeded their initial period of usefulness. Subscribers who engage in such applications must ensure that those applications can use expired certificates, or manage the storage of their data such that the original signatures and encryptions are not used.

Subscriber public keys in code signing certificates have a maximum usage period of <number> years. The private keys corresponding to the public keys in these certificates have a maximum usage period of <number> years.

For OCSP responders operating under this policy and all other subscriber public keys, the maximum usage period is three years. Subscriber signature private keys have the same usage period as their corresponding public key. The usage period for subscriber key management private keys is not restricted.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

CA activation data may be user-selected (by each of the multiple parties holding that activation data). If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

RA and subscriber activation data may be user-selected. The strength of the activation data shall meet or exceed the requirements for authentication mechanisms stipulated for Level 2 in [FIPS 140] . If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data shall be either:

- memorized;
- biometric in nature; or
- recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

6.5.1.1 Access Control

Access to information such as sensitive details about customer accounts, passwords, and ultimately, CA-related private keys should be carefully guarded, along with the machines housing such information.

6.5.1.1.1 Access Control Policy and Procedures

The CA shall create and document roles and responsibilities for each employee job function in the CPS. The CA shall create and maintain a mapping of these roles and their associated responsibilities to specific employees and their accounts on CA systems.

6.5.1.1.2 Account Management

Information system account management features shall ensure that users access only that functionality permitted by their role or function. All account types with access to information systems shall be documented along with the conditions and procedures to follow in creating new accounts. Groups and roles shall have a documented relationship to the business or mission roles involved in operating the CA.

Section 5.2.1 of this document defines roles and job functions for personnel that the CA will use when defining access control mechanisms. The CA shall employ the principle of least privilege when creating users and assigning them to groups and roles; membership to a group or role is granted shall be justified based upon business need. The CA shall take appropriate action when a user no longer requires an account, their business role changes, or the user is terminated or transferred. Periodically, the CA shall review all active accounts to match active authorized users with accounts, and disable any accounts no longer associated with an active authorized user.

To assist with the management of the information system accounts, automated systems shall assist in maintaining access for only those users who are still authorized to use the information system. After an

extended period of inactivity, an account shall be automatically disabled and attempts to access any deactivated account shall be logged.

All account administration activities shall be logged and made available for inspection by appropriate security personnel. Account administration activities that shall be audited include account creation, modification, enabling, disabling, group or role changes, and removal actions.

The use of shared/group and guest/anonymous accounts for logon to information systems shall be prohibited.

6.5.1.1.3 Least Privilege

In granting rights to accounts and groups, the CA shall employ the principle of least privilege, allowing only authorized access for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. The CA shall explicitly authorize access to accounts and groups for controlling security functions and security-relevant information. The CA shall authorize access to privileged commands and features of information systems only for specific, organization-defined compelling operational needs and documents the rationale for such access. The CA shall require that users of information systems with access to administrative privileges to utilize non-privileged accounts or roles when accessing non-privileged functions (such as reading email).

6.5.1.1.4 Access Control Best Practices

Instruction: This section should identify appropriate security best practices related to the use and maintenance of user and administrative accounts. The CP writer may, for example, require that CA systems notify users of their previous successful logon, and implement automated session locks after periods of inactivity. This section may also identify other mitigations, such as limiting browser use by administrators so that it is only associated with specific administrative activities requiring a browser in the system, blocking browser access of publicly available websites.

6.5.1.1.5 Permitted Actions without Identification or Authentication

The organization shall document a specific list of actions that can be performed on specifically enumerated information systems without identification or authentication, such as retrieving or verifying a published CRL from an Internet-accessible server or accessing a publicly available website. Furthermore, the organization shall document and provide supporting rationale in its security policy and procedures an enumerated list of user actions and systems not requiring identification or authentication (i.e., anonymous access).

6.5.1.2 System Integrity

6.5.1.2.1 System Isolation and Partitioning

CA systems shall be configured, operated, and maintained so as to ensure the continuous logical separation of processes and their assigned resources. This separation shall be enforced by

- physical and/or logical isolation mechanisms, such as dedicated systems or virtualization
- protecting an active process and any assigned resources from access by or interference from another process

- protecting an inactive process and any assigned resources from access by or interference from an active process
- ensuring that any exception condition raised by one process will have no lasting detrimental effect on the operation or assigned resources of another process

All trusted components should be logically separated from each other, and shall be logically separated from any untrusted components of the CA system. The CPS shall document how it this logical isolation of components is accomplished.

Security critical processes shall be isolated from processes that have external interfaces. For example the CA signing processes shall be isolated from registration processes. The CPS shall outline how security critical processes are protected from interference by externally facing processes.

If there are system resources shared amongst trusted and/or untrusted processes, the underlying system(s) shall prevent any unauthorized and unintended information transfer between processes via those shared system resources.

The CA shall develop and document controlled procedures for transferring software updates, configuration files, certificate requests, and other data files between trusted components.

6.5.1.2.2 Malicious Code Protection

The CA system shall employ malicious code protection mechanisms to mitigate the risk of malicious code on CA system components. Malicious code on trusted CA components could allow an attacker to issue fraudulent certificates, create a rouge intermediate or signing CA server, or compromise the availability of the system.

CA system components running standard operating systems that are not air-gapped from the Internet shall employ host-based anti-malware tools to detect and prevent the execution of known malicious code. These tools shall be configured to automatically scan removable media when it is inserted, as well as files received over the network. Introduction of removable media shall not cause automatic execution of any software residing on the media.

Anti-malware tools employed by a CA shall be properly maintained and updated by the CA. Anti-malware tools on networked systems shall be updated automatically as updates become available, or CA system administrators shall push updates to system components on a <weekly> basis. Anti-malware tools may be employed on air-gapped systems. However, without sufficient technical and procedural controls, the processes for updating these tools could provide an attacker with a means for spreading malicious code to these air-gapped systems. If anti-malware tools are employed on air-gapped systems, the CA shall document in the CPS how these tools will be updated, including mitigations intended to reduce the risks of spreading malware and exfiltration of data off of compromised CA systems.

Anti-malware tools shall alert system administrators of any malware detected by the tools.

On system components that do not implement host-based anti-malware tools, the CA shall identify and employ other malicious code protection mechanisms to prevent the execution of malicious code, detect infected files or executables, and remediate infected systems. These mechanisms could include, but are not limited to, compensating physical protection on hosts, network-based malware detection tools at boundary points, application whitelisting, and manually scanning removable media by trusted CA personnel. The CA shall document all malware protection mechanisms in the CPS.

6.5.1.2.3 Software and Firmware Integrity

The CA shall employ technical and procedural controls to prevent and detect unauthorized changes to firmware and software on CA systems. Access control mechanisms and configuration management processes (see Section 6.5.1.1 and 6.6.2) shall ensure that only authorized system administrators are capable of installing or modifying firmware and software on CA systems.

Root and subordinate CA servers shall implement automated technical controls to prevent and detect unauthorized changes to firmware and software. These controls may include signature verification prior to firmware/software installation or execution (such as firmware protections that comply with [SP800-147] or [SP800-147B]), or hash-based white-listing of executables. Unauthorized software or firmware detected by these mechanisms should be blocked from executing. Any instances of unauthorized firmware or software detected by the system shall be logged, and system administrators shall be notified of these events.

6.5.1.2.4 Information Protection

The CA shall protect the confidentiality and integrity of sensitive information stored or processed on CA systems that could lead to abuse or fraud. For example, the CA shall protect customer data that could allow an attacker to impersonate a customer. The CA shall employ technical mechanisms to prevent unauthorized changes or accesses to this information, such as access control mechanisms that limit which users are authorized to view or modify files. Sensitive information stored on devices that are not physically protected from potential attackers shall be stored in an encrypted format, using a NIST-approved encryption algorithm and mode of operation.

6.5.2 Computer Security Rating

No Stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The system development controls address various aspects related to the development and change of the CA system through aspects of its life-cycle.

The CA system shall be implemented and tested in a non-production environment prior to implementation in a production environment. No change shall be made to the production environment unless the change has gone through the change control process as defined for the system baseline.

In order to prevent incorrect or improper changes to the CA system, the CA system shall require multi-party control for access to the CA system when changes are made.

For any software developed by the CA, evidence shall be produced relating to the use of a defined software development methodology setting out the various phases of development, as well as implementation techniques intended to avoid common errors to reduce the number of vulnerabilities. Automated software assurance (i.e. static code analysis) tools shall be used to catch common error conditions within developed code. For compiled code, all compiler warnings shall be enabled and addressed or acknowledged to be acceptable. Input validation shall be performed for all inputs into the system.

All data input to CA system components from users or other system components shall be validated prior to consumption by the receiving entity. Validating the syntax and semantics of system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match the expected definitions for format and content.

6.6.2 Security Management Controls

A list of acceptable products and their versions for each individual CA system component shall be maintained and kept up-to-date within a configuration management system. Mechanisms and/or procedures shall be in operation designed to prevent the installation and execution of unauthorized software. A signed whitelist of the acceptable software for the system should be one of the ways to control the allowed software. A CA system shall have automated mechanisms to inventory on at least a daily basis software installed on a system and alert operators if invalid software is found.

To reduce the available attack surface of a CA system, only those ports, protocols, and services that are necessary to the CA system architecture are permitted to be installed or operating. The CA system shall maintain a list of ports, protocols, and services that are necessary for the correct function of each component within the CA system. There shall be automated mechanisms to monitor the running processes and open ports against the permitted list.

To validate the integrity of the CA system, automated tools that validate all static files on a component shall be in operation to notify operators when a protected file has changed.

The CA system shall establish and document mandatory configuration settings for all information technology components which comprise the CA system. All configuration settings capable of automated assessment shall be validated to be set according to the guidance contained within a documented security configuration checklist on at least daily basis for powered on systems or next power-on for systems which are not left powered-on.

6.6.3 Life Cycle Security Controls

For flaw remediation, the CA shall scan all CA systems for vulnerabilities using at least one vulnerability scanner every <time period>. The use of multiple scanners on the most sensitive systems is strongly encouraged.

Each vulnerability found shall be entered into a vulnerability tracking database, along with the date and time of location, and shall be remediated within <72 hours>. Remediation shall be entered into the vulnerability database as well (including date and time).

The CA shall monitor relevant notification channels on a <daily> basis for updates to packages installed on CA systems (including networking hardware). CAs shall have a plan for receiving notification of software and firmware updates, for obtaining and testing those updates, for deciding when to install them, and finally for installing them without undue disruption. For critical vulnerabilities, the CA shall evaluate and install the update within <24 hours>. For less critical vulnerabilities, the CA shall evaluate each package to determine whether an update is required, and if so, that update shall be applied to all affected CA systems within <48 hours>. A log shall be kept of the notifications, the decision to apply/not apply including reason, and the application of relevant updates/patches.

From time to time, the CA may discover errors in configuration files, either because of human error, source data error, or changes in the environment which have made an entry erroneous. The CA shall correct such errors within <24 hours> of discovery, and shall document the reason for the error, and the

associated correction.

In no case should a remediation cause unavailability of revocation information.

6.7 Network Security Controls

The various components of a CA are, for the most part, connected to each other and their customers via various forms of networks. While it is necessary for connections to customers and administrative systems, care shall be taken to ensure those connections do not adversely impact the security of those components. Guidelines for effective CA networking security are discussed in the following sections.

6.7.1 Isolation of Networked Systems

Isolation is the ability for components of a system to cooperate without the possibility of one compromising the other's function either by accident or due to malicious intent. For systems connected to more public networks, this requirement is even stronger since by being so connected the number of systems is much higher, thereby raising the probability of mistakes or the presence of attackers. Within a distinct system, components are isolated from each other through system isolation (See Section 6.5.1.2.1). Networked systems also require logical, and sometimes physical, isolation from one another.

CAs which are connected to networks are, thus, exposed to potential attackers. Communication channels between the network-connected CA components and the trusted CA processing components shall be protected against attack. Furthermore, information flowing into these CA components from the network-connected CA components shall not lead to any compromise or disruption of these components.

The components of a CA requiring direct network connections shall be minimized. Those networked components shall be protected from attacks through the use of firewalls to filter unwanted protocols (utilizing access rules, whitelists, blacklists, protocol checkers, etc., as necessary). Similarly, some form of data leak prevention shall be employed to detect inappropriate leakage of sensitive information.

6.7.2 Boundary Protection

Boundary protection is discussed in the context of four zone types. The zones are not assumed to be nested. They may be interconnected, but are independent. Zone boundaries are defined by limits of authority over the security of the data processed within the boundary. Interconnection of two zones, even at the same protection level, must be done in a way that respects the different authorities of the two zones. The zones are:

- Special Access Zone (SAZ) - highly controlled network area for processing and storage of especially high value data. It should be assumed that a network in this zone is not interconnected to any other network.
- Restricted Zone (RZ) - controlled network area for sensitive data processing and storage.
- Operations Zone (OZ) - network area containing systems for routine business operations.
- Public Zone (PZ) - any network area that is not behind a protective boundary controlled by the organization. Includes the public Internet and the public telephone network. Since there is no presumed control over the Public Zone, there are no requirements for boundary protection.

6.7.2.1 PKI Network Zones Overview

A Root CA is expected to reside in a Special Access Zone with no network connection to any other network at all. Subordinate CAs are expected to reside in one or more Restricted Zones, with connections

allowed from the Public Zone for RA Agent access and from the Operations Zone for business function access.

The RA Server is expected to reside in a Restricted Zone distinct from the Restricted Zone occupied by the CA Signing Servers. The RA Agent may reside in a Restricted, Operations, or Public Zone. While the RA Agent may use special hardware and software to accomplish their tasks, the organization will have no control over the RA Agent's workstation's network connection if it operates in the Public Zone. The data must be self-protecting or session protected as it leaves the RA Agent's workstation.

The following sections describe the boundary of each zone type in the context of an extended CA, including connections to systems that support but are not part of the CA.

6.7.2.2 Special Access Zone Boundary

A SAZ has no physical nor logical interconnection to any other network.

- Physical boundary protection measures shall include checks for network elements (cables, routers, wireless equipment) that indicate interconnection.
- Incoming communication is limited to certificate signing requests and system maintenance data.
- Outgoing communication is limited to signed certificates, CRLs, and any data related to monitoring and audit.
- Communication shall be accomplished by means of write-once media or media that is sanitized on first use and between uses. Media shall be scanned after writing. The sanitization and scanning shall take place on a device isolated and designated solely for this purpose.
- Auditing functions shall be enabled on systems in the SAZ, according to the requirements in Section 5.4.
- Systems shall be physically isolated to separate platform instances and uniquely identified on each subnet within SAZ boundary with managed interfaces.

6.7.2.3 Restricted Zone Boundary

An RZ has physical interconnections to other RZs, OZs, and potentially the PZ.

- Physical interconnections must be documented as to where they exist, for what purpose, and what protections are provided.
- All physical systems shall identify and limit all systems to managed interfaces.
- All interconnections must be filtered based on origin, destination, and type.
- Physical boundary protection measures shall include checks for network elements (cables, routers, wireless equipment) that indicate unauthorized interconnection.
- Physical boundary protection devices shall fail securely in the event of an operational failure.
- Connections with other RZs may be firewalled interconnections that maintain the security posture of each RZ.
- Connections with OZs must be limited to specific protocols, and connections digitally authenticated. If there is a Wireless Access Point in the OZ, a VPN Gateway shall be used to connect to the Restricted Zone.
- Confidentiality shall be provided depending on the sensitivity of the information transferred and the route of the connection.
- Connection with the PZ must be made through a bastion host that is hardened for exposure to a hostile network environment. Such bastion hosts must be minimized in number and documented as to location, purpose, and system and service configuration.

- Firewalls shall allow only those protocols necessary to perform a function and only from recognized network origins by denying network traffic by default and allowing network traffic only by exception (i.e., deny all, permit by exception).
- All communications shall be source authenticated.
- Incoming communications shall be limited to certificate signing requests, CRL requests, key recovery requests, key escrow messages, revocation requests, responses from support systems (e.g., from a directory), and system maintenance data.
- Outgoing communications shall be limited to signed certificates, CRLs, key recovery data, revocation request responses, requests for subscriber authentication and authorization data, and any data related to monitoring and audit.
- Monitoring and auditing functions shall be enabled on the systems in the RZ, including network components where appropriate, according to the requirements in Sections 5.4 and 6.7.5.
- Indications that boundary protections have failed must be dealt with urgently (see Section 5.7).
- Wireless access points shall NOT be allowed in the Restricted Zone at any time.

6.7.2.4 Operational Zone Boundary

An OZ has physical interconnections to other OZs, RZs, and the PZ.

- Physical interconnections must be documented as to where they exist, for what purpose, and what protections are provided.
- All interconnections must be filtered based on origin, destination, and type.
- Physical boundary protection measures shall include checks for network elements (cables, routers, wireless equipment) that indicate unauthorized interconnection.
- Physical boundary protection devices shall fail securely in the event of an operational failure.
- Connections with RZs shall be driven by the RZ boundary protection requirements.
- Connections with other OZs may be firewalled router interconnections that maintain the security posture of each OZ.
- Connections with the PZ must be limited to specific protocols, and connections digitally authenticated.
- Confidentiality of any interconnection shall be provided depending on the sensitivity of the information transferred and the route of the connection.
- Firewalls shall allow only those protocols necessary to perform a function and only from recognized network origins by denying network traffic by default and allowing network traffic by exception (i.e., deny all, permit by exception).
- All communications shall be source authenticated.
- Incoming and outgoing communications shall be limited to data related to the business of the organization, system maintenance data, and any data related to monitoring and audit.
- Monitoring and auditing functions shall be enabled on the systems in the OZ, including network components where appropriate, according to the requirements in Sections 5.4 and 6.7.5.
- Indications that boundary protections have failed must be dealt with promptly (see Section 5.7).
- Wireless Access Points should NOT be allowed in the OZ unless the radio frequency can be physically contained with high assurance to systems isolated in the OZ of the building structure.

6.7.3 Availability

Certificate request and issuance services need to be available, but can tolerate some down time.

Revocation services, which include the request for revocation as well as the advertisement of revoked certificates, need to be highly available. If revocation information is not available, or if revocation

information is inaccurate, then a Relying Party could be easily convinced to trust a revoked certificate. See Section 2.2.1 for requirements on publication availability.

6.7.3.1 Denial of Service Protection

CA systems shall be configured, operated, and maintained to maximize uptime and availability. Scheduled downtime shall be announced to Subscribers.

CAs shall state acceptable methods to request revocation in their CPS. At least one of those methods shall be out of band (i.e. network connectivity is not required).

CAs shall state in their CPSs their guaranteed availability for revocation information and how they achieve it. CAs shall make revocation information available in at least one form that can be used in a cached, offline manner. The CA revocation information availability required shall be stated in its CPS

CAs shall take reasonable measures to protect certificate request and issuing services from known DoS attacks. The CA request and issuing availability required by a Subscriber application shall be stated in its CPS

Revocation services need to configured and deployed in such a manner and capacity that overall availability shall be maintained at a minimum of <99.99% (52 minutes/year)>, with no single outage lasting longer than <5> minutes. Additionally, such services shall be homed in a minimum of two geographically independent locations with no single-points of failure (SPOFs – e.g., same backbone provider) which could affect availability.

6.7.3.2 Public Access Protections

"Public Access" in this section shall mean widespread, anonymous access.

Revocation information shall be available to Relying Parties, but need not be publically available. The CA shall make CRL information available to the expected relying parties. CAs shall state in their CPS how they deliver certificates to Subscribers and Relying Parties.

The CA shall make its CPS summary either available upon request, or publically available.

6.7.4 Communications Security

This section is divided into three sections: Intra-CA communications, CA to RA communications, and RA to Subscriber communications. While communications security is necessary at every stage, the threats, vulnerabilities, and technological capabilities change depending on the environment.

Intra-CA Communications: This stage includes communications between the components that make up the certificate manufacturing and signing function. At minimum this includes the certification authority workstation and hardware security module. If the CA is part of a managed network, it may also include a domain controller, directory (e.g., LDAP server), and perhaps other components.

CA to RA Communications: RAs are generally co-located with Subscribers, so communications between the RA and CA will typically be inter-network. Although this could be accomplished by using a virtual private network connection, that level of relationship between the RA and CA is unusual and not assumed.

RA to Subscriber Communications: The fewest number of assumptions can be made about the RA to Subscriber environment, because of the variety of models for this relationship, and the relative lack of control over the Subscriber. Where there is no RA, this section shall be construed to provide CA to Subscriber communications security requirements.

6.7.4.1 Transmission Integrity

Source authentication and integrity mechanisms shall be employed to all certificate request, manufacture, and issuance communications, including all related services irrespective of whether those services are hosted on the same or different platform than the CA workstation. Communications between CAs and RAs shall be mutually authenticated to detect changes to information during transmission.

Source authentication for RA to Subscriber communications may employ either online (cryptographic) or offline methods. Offline RA to Subscriber communications shall be protected by traditional means that are legally sufficient (e.g., ink signatures on paper). Initial Subscriber data that has been collected in an unauthenticated or mutable manner shall be verified by the RA before the certificate request is created.

6.7.4.2 Transmission Confidentiality

Intra-CA communications that cross the physical protection barrier of the certificate-signing portion of the CA system shall be confidentiality-protected. Services used by the CA system that are not administered by the CA administrative staff shall provide protection commensurate with any applicable CP.

Confidentiality of Subscriber data shall be maintained. CA to RA communications shall employ encryption to prevent unauthorized disclosure of information during transmission. The level of protection for RA to Subscriber communications shall be determined by the Subscriber (or the Subscriber's organization); in any case, the RA shall be prepared to employ typical techniques for Internet confidentiality (e.g., single-side authenticated TLS).

6.7.4.3 Network Disconnect

Network connection lifetimes between co-located services are driven by the traffic between them. Connections should be terminated after a period of inactivity that is defined in the CA's CPS.

Network connections between CAs, RAs, and Subscribers shall be terminated at the end of the session or after a period of inactivity. The length of the period of inactivity is defined in the CA's CPS. Keep-alive and quick-reconnect mechanisms should not be employed, so that message replay and session hijacking are avoided.

6.7.4.4 Cryptographic Key Establishment and Management

Cryptographic key management includes all aspects of cryptographic key life cycle: key generation, distribution, storage, access and destruction for both symmetric and asymmetric keys.

Key generation and management shall be performed in cryptographic modules which are validated to [FIPS-140] Level 1 or higher. Keys that are backed up for business continuity shall have protection comparable to the operational key. All cryptographic key management processes shall be described in the CA's CPS.

The CA service shall employ key protection mechanisms implemented in a cryptographic module

validated to [FIPS 140] Level 1 or higher. RAs shall employ key protection mechanisms implemented in a [FIPS 140] Level 2 or higher validated hardware device (e.g., smart token).

Keys that protect the integrity and confidentiality of an enrollment session shall be generated and managed using cryptographic mechanisms implemented in a [FIPS 140] Level 1 (or higher) validated module.

6.7.4.5 Cryptographic Protection

Cryptographic mechanisms implemented in a [FIPS 140] Level 1 (or higher) cryptographic module shall be employed to detect changes to information during transmission of Intra-CA communications.

Communications between the CA and RA systems shall use cryptographic mechanisms that are implemented in a [FIPS 140] Level 1 (or higher) validated module.

Cryptographic processes for RA to Subscriber communications shall be implemented in a [FIPS 140] Level 1 (or higher) validated module.

6.7.4.6 Session Authenticity

For stateless connections, a unique, random session identifier for each session shall be generated. Session identifiers shall be invalidated at logout to preserve session authenticity. A logout capability shall be provided with an explicit logout message that indicates the reliable termination of authenticated communications sessions. The CA will only recognize session identifiers generated by authorized entities.

For RA to Subscriber communications, session identifiers shall not be reused. The parties involved in a session shall have a clear session termination capability, and shall receive explicit notification that a session has been terminated.

6.7.5 Network Monitoring

The CA shall be monitored to detect attacks and indicators of potential attacks. Examples of this include intrusion detection tools.

6.7.5.1 Events and Transactions to be Monitored

The CA shall identify a list of essential information, transaction types and thresholds that indicate potential attacks. These events should include:

- Bandwidth thresholds
- Inbound and outbound communication events and thresholds
- Unauthorized network services
- CPU usage thresholds
- Certificate request thresholds from a single RA
- Access Control thresholds

6.7.5.2 Monitoring devices

A CA shall deploy intrusion detection tools or other monitoring devices with the CA to collect intrusion information and at ad hoc locations within the system to track specific types of transactions of interest to

the organization. These monitoring devices shall be configurable to react to specific indications of increased risk or to comply with law enforcement requests. The devices shall alert security personnel when suspected unauthorized activity is occurring. These devices shall be network-based and should be also host-based. The devices shall NOT be bypassable by non-privileged users. The CA should utilize automated tools to support near real-time analysis of events and these tools should be integrated into access control and flow control mechanisms for rapid response to attacks.

6.7.5.3 Monitoring of Security Alerts, Advisories, and Directives

A CA shall monitor information system security alerts, advisories, and directives on an ongoing basis. The CA shall generate and disseminate internal security alerts, advisories, and directives as deemed necessary. The CA should employ automated mechanisms to make security alert and advisory information available throughout the organization as needed. The CA shall implement security directives in accordance with established time frames, or notifies the compliance auditor of the degree of noncompliance.

6.7.6 Remote Access/External Information Systems

6.7.6.1 Remote Access

For operational reasons, there may be a need to perform remote management of some CA resources. The requirements in this section are meant to allow remote management while maintaining the desired security posture.

6.7.6.2 Bastion Host

All access to CA systems in a RZ shall be mediated by a bastion host (i.e. a machine that presents a limited interface for interaction with the other elements of the CA). No direct access is permitted. The bastion host shall be patched regularly, maintained, and shall only run applications required to perform its duties. The Bastion Hosts shall be located between the RZ where the CA is located and the zone where the CA Operations Staff are located. No remote access is permitted with SAZ systems.

6.7.6.3 Documentation

The CA shall document allowed methods of remote access to CA systems, including usage restrictions and implementation guidance for each allowed remote access method.

6.7.6.4 Logging

Logging shall be performed on the bastion host for each remote access session with the CA, consistent with Section 5.4. In particular, logs should include date and time of the connection, the authenticated identity of the requestor, the IP address of the remote system and the commands sent to the bastion host. Logs shall be maintained on a corporate audit server. Time on the bastion host shall be synchronized with an authoritative time source.

6.7.6.5 Automated Monitoring

Automated monitoring shall be performed on all remote sessions with the bastion host, and on all interactions between the bastion host and other CA systems. Upon detection of unauthorized access, the CA shall terminate the connection and log the event.

6.7.6.6 Security of Remote Management System

Machines used for remote access to the CA system shall be either corporately managed (including patching) or shall be a machine dedicated to that purpose. In particular, it shall not be used as a personal machine for the remote user. The machine shall be maintained at the same level as the machines that it accesses (i.e. all policies on patching, virus scanning, etc. that are levied on the target systems shall apply to this machine as well). The CA should make use of Network Access Control technology to check the security posture of the remote machine prior to connecting it to the network. Remote Management of the CA system shall be the only use of Remote Access.

6.7.6.7 Authentication

Any machine used to access CA systems remotely shall require two or more factors of authentication. In particular, a hardware token shall be required. Authentication shall occur between the remote machine and the bastion host.

6.7.6.8 Communications Security for Remote Access

All communications between the remote access host and the CA system shall be protected by [FIPS 140] validated cryptography, as required for CA to RA communications in Section 6.7.4.5. Session identifiers shall be invalidated at logout to preserve session authenticity, as described in section 6.7.4.6, Session Authentication.

6.7.7 Penetration Testing

Penetration testing exercises both physical and logical security controls. Regularly performing this testing will allow a CA to mitigate and avoid vulnerabilities in their systems.

The CA System shall conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems. Penetration testing shall occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.

A standard method for penetration testing consists of:

- pretest analysis based on full knowledge of the target system;
- pretest identification of potential vulnerabilities based on pretest analysis;
- testing designed to determine exploitability of identified vulnerabilities.

Detailed rules of engagement shall be agreed upon by all parties before the commencement of any penetration testing scenario. These rules of engagement are correlated with the tools, techniques, and procedures that are anticipated to be employed by threat-sources in carrying out attacks. An organizational assessment of risk guides the decision on the level of independence required for penetration agents or penetration teams conducting penetration testing. Vulnerabilities uncovered during penetration testing shall be incorporated into the vulnerability remediation process.

6.8 Time-Stamping

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events (see section 5.4.1).

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Certificates issued by a CA under this policy shall conform to the <profile document reference>.

Instruction: Although it is possible to specify all of the requirements for certificate fields and values in this section, it is more common to include a reference here to a separate document that includes those requirements. That document, called a "profile" because it specifies acceptable options and values from a more general document, is written by technical staff and often based on a standard such as [RFC 5280]. The sections here are provided for assessment by a knowledgeable but non-expert reader; these sections must be edited to agree with the profile document. The profile document must be carefully written to provide the necessary security and interoperability features.

7.1.1 Version Number(s)

The CA shall issue X.509 v3 certificates (populate version field with integer "2").

7.1.2 Serial Numbers

Shall be a positive unique integer**,** shall not be longer than 20 octets. Shall contain at least <20 bits> of random.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use the following OIDs for signatures:

id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
id-RSASSA-PSS	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}
ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2}
ecdsa-with-Sha384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3}

Where certificates are signed using RSA with Probabilistic Signature Scheme (PSS) padding, the OID is independent of the hash algorithm; the hash algorithm is specified as a parameter. RSA signatures with PSS padding may be used with the hash algorithms and OIDs specified below:

id-sha256	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1}

Certificates issued under this CP shall use the following OIDs to identify the algorithm associated with the subject key:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
Id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public key-type (2) 1}
id-ecDH	{iso(1) identified-organization(3) certicom(132) schemes(1) ecdh(12)}
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}

Where the certificate contains an elliptic curve public key, the parameters shall be specified as one of the following named curves:

ansip256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}
ansip384r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 }

7.1.4 Name Forms

The subject field in certificates issued under this policy shall be populated with an X.500 distinguished name as specified in section 3.1.1.

The issuer field of certificates issued under this policy shall be populated with a non-empty X.500 Distinguished Name as specified in section 3.1.1.

7.1.5 Subject Alternate Name (SAN)

See Section 3.1.

7.1.6 Key Usage

This extension shall be marked as critical. Certificates shall assert the minimum required for functionality. Signature certificates shall assert *digitalsignature*. Encryption certificates shall assert either *keyencipherment* or *keyagreement*. CA certificates shall assert *digitalsignature, keyCertSign* and *CRLSign*

7.1.7 Extended Key Usage

This extension shall be marked as noncritical. Certificates shall assert the minimum number required for functionality. The *anyExtendedEKU* shall not be asserted.

7.1.8 Name Constraints

The CAs should assert name constraints in CA certificates.

7.1.9 Basic Constraints

CA certificates shall mark this extension critical. A path length constraint should be set to <2>.

7.1.10 Certificate Policy Object Identifier

Certificates issued under this CP shall assert the following OID(s):

<id-policy-defined-in-this-document>::=<OID>

Instruction: This section spells out how the requirements of this certificate policy are asserted in certificates. The OID specified above is the one from Section 1.2. If this document defines more than one certificate policy (e.g., defines more than one level of assurance), then they would be listed here with a requirement to include the OID matching the policy followed during certificate issuance. Very rarely, policy OIDs from other documents may be included as well, for instance a certificate may meet the requirements for a departmental business function as well as requirements for organizational network authentication. It should be kept in mind that certificate policy OIDs are an assertion to the user of the certificate (i.e., the Relying Party), and should reflect all that is true and only that which is true about the certificate.

7.1.11 Usage of Policy Constraints Extension

The CAs may assert policy constraints in CA certificates.

7.1.12 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP shall not contain policy qualifiers.

7.1.13 Processing Semantics for the Critical Certificate Policies Extension

Certificates issued under this policy shall not contain a critical certificate policies extension.

7.2 CRL Profile

CRLs issued by a CA under this policy shall conform to the CRL profile specified in <profile document reference>.

7.2.1 Version Number(s)

The CAs shall issue X.509 Version two (2) CRLs.

7.2.2 CRL and CRL Entry Extensions

Detailed CRL profiles addressing the use of each extension are specified in <profile document reference>.

7.3 OCSP Profile

Certificate status servers (CSSs) operated under this policy shall sign responses using algorithms designated for CRL signing.

CSSs shall be able to process SHA-1 hashes when included in the CertID field and the keyHash in the responderID field.

7.3.1 Version Number(s)

CSSs operated under this policy shall use OCSP version 1.

7.3.2 OCSP Extensions

Critical OCSP extensions shall not be used.

8 Compliance Audit and Other Assessments

CAs shall have a compliance audit mechanism in place to ensure that the requirements of their CPS are being implemented and enforced.

This specification does not impose a requirement for any particular assessment methodology.

8.1 Frequency or Circumstances of Assessment

CAs and RAs shall be subject to a periodic compliance audit at least once per year.

8.2 Qualifications of Assessor

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CA's CPS and this CP. The compliance auditor must perform such compliance audits as a regular ongoing business activity. In addition to the previous requirements, the auditor must be a certified information system auditor (CISA) or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor either shall be a private firm that is independent from the entities (CA and RAs) being audited, or it shall be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. To insure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's CA Facility or certificate practices statement. The Policy Authority shall determine whether a compliance auditor meets this requirement.

8.4 Topics Covered by Assessment

The purpose of a compliance audit shall be to verify that a CA and its recognized RAs comply with all the requirements of the current versions of this CP and the CA's CPS. All aspects of the CA/RA operation shall be subject to compliance audit inspections.

8.5 Actions Taken as a Result of Deficiency

When the compliance auditor finds a discrepancy between the requirements of this CP or the stipulations in the CPS and the design, operation, or maintenance of the PKI Authorities, the following actions shall be performed:

- The compliance auditor shall note the discrepancy
- The compliance auditor shall notify the parties identified in section 8.6 of the discrepancy
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the Policy Authority

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the Policy Authority may decide to temporarily halt operation of the CA or RA, to revoke a certificate issued to the CA or RA, or take other actions it deems appropriate. The Policy Authority will develop procedures for making and implementing such determinations.

8.6 Communication of Results

An Audit Compliance Report shall be provided to the entity responsible for CA operations. The Audit Compliance Report and identification of corrective measures shall be provided to Policy Authority within <30> days of completion. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

Section 2.2 of this policy requires that CA certificates be publicly available. CAs operating under this policy must not charge additional fees for access to this information.

9.1.3 Revocation or Status Information Access Fees

CAs operating under this policy must not charge additional fees for access to CRLs and OCSP status information.

9.1.4 Fees for other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

This CP contains no limits on the use of certificates issued by CAs under the policy. Rather, entities, acting as relying parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

The CA shall protect the confidentiality of sensitive business information stored or processed on CA systems that could lead to abuse or fraud. For example, the CA shall protect customer data that could allow an attacker to impersonate a customer.

CA information not requiring protection may be made publicly available. Public access to organizational information shall be determined by the respective organization.

9.3.1 Scope of Confidential Information

No stipulation.

9.3.2 Information not within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

No stipulation.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The CA shall develop, implement and maintain a privacy plan. The privacy plan shall document what personally identifiable information is collected, how it is stored and processed, and under what conditions the information may be disclosed.

9.4.2 Information Treated as Private

CAs shall protect all subscriber personally identifying information from unauthorized disclosure. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. The contents of the archives maintained by CAs operating under this policy shall not be released except as allowed by the privacy plan.

9.4.3 Information not Deemed Private

Information included in certificates is not subject to protections outlined in section 9.4.2.

9.4.4 Responsibility to Protect Private Information

Sensitive information must be stored securely, and may be released only in accordance with other stipulations in section 9.4.

9.4.5 Notice and Consent to Use Private Information

The CA is not required to provide any notice or obtain the consent of the subscriber in order to release private information in accordance with other stipulations of section 9.4.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The CA shall not disclose private information to any third party unless authorized by this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction.

9.4.7 Other Information Disclosure Circumstances

None.

9.5 Intellectual Property Rights

The CA will not knowingly violate intellectual property rights held by others.

9.6 Representations and Warranties

The Policy Authority shall—

- Approve the CPS for each CA that issues certificates under this policy;
- Review periodic compliance audits to ensure that CAs are operating in compliance with their approved CPSs;
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under this CP;
- Revise this CP to maintain the level of assurance and operational practicality;
- Publicly distribute this CP; and
- Coordinate modifications to this CP to ensure continued compliance by CAs operating under approved CPSs.

9.6.1 CA Representations and Warranties

CAs operating under this policy shall warrant that their procedures are implemented in accordance with this CP, and that any certificates issued that assert the policy OIDs identified in this CP were issued in accordance with the stipulations of this policy.

A CA that issues certificates that assert a policy defined in this document shall conform to the stipulations of this document, including—

- Providing a CPS, as well as any subsequent changes, for conformance assessment.
- Maintaining its operations in conformance to the stipulations of the CPS.
- Ensuring that registration information is accepted only from approved RAs operating under an approved CPS.
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates.
- Revoking the certificates of subscribers found to have acted in a manner counter to their obligations in accordance with section 9.6.3.
- Operating or providing for the services of an on-line repository, and informing the repository service provider of their obligations if applicable.

9.6.2 RA Representations and Warranties

An RA that performs registration functions as described in this policy shall comply with the stipulations of this policy, and comply with a CPS approved by the Policy Authority for use with this policy. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities. An RA supporting this policy shall conform to the stipulations of this document, including—

- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate.

- Ensuring that obligations are imposed on subscribers in accordance with section 9.6.3, and that subscribers are informed of the consequences of not complying with those obligations.

9.6.3 Subscriber Representations and Warranties

A subscriber (or AOR for device certificates) shall be required to sign a document containing the requirements the subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate.

Subscribers shall—

- Accurately represent themselves in all communications with the PKI authorities.
- Protect their private key(s) at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures.
- Promptly notify the appropriate CA upon suspicion of loss or compromise of their private key(s). Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS.
- Abide by all the terms, conditions, and restrictions levied on the use of their private key(s) and certificate(s).

9.6.4 Relying Parties Representations and Warranties

This CP does not specify the steps a relying party should take to determine whether to rely upon a certificate. The relying party decides, pursuant to its own policies, what steps to take. The CA merely provides the tools (i.e., certificates and CRLs) needed to perform the trust path creation, validation, and CP mappings that the relying party may wish to employ in its determination.

9.6.5 Representations and Warranties of Other Participants

None.

9.7 Disclaimers of Warranties

CAs operating under this policy may not disclaim any responsibilities described in this CP.

9.8 Limitations of Liability

No stipulation

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

The CP shall document the term for which the CP is effective.

9.10.2 Termination

The CP shall document under what conditions the CP may be terminated..

9.10.3 Effect of Termination and Survival

The requirements of this CP remain in effect through the end of the archive period for the last certificate issued.

9.11 Individual Notices and Communications with Participants

The Policy Authority shall establish appropriate procedures for communications with CAs operating under this policy via contracts or memoranda of agreement as applicable.

For all other communications, no stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

The Policy Authority shall review this CP at least once every year. Corrections, updates, or changes to this CP shall be publicly available. Suggested changes to this CP shall be communicated to the contact in section 1.5.2; such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.2 Notification Mechanism and Period

No stipulation.

9.12.3 Circumstances under which OID must be Changed

OIDs should be changed if there is a change in the CP that reduces the level of assurance provided.

9.13 Dispute Resolution Provisions

The Policy Authority shall facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this policy.

9.14 Governing Law

No stipulation.

9.15 Compliance with Applicable Law

All CAs operating under this policy are required to comply with applicable law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 9.12.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.

Appendix A—Acronyms

Selected acronyms and abbreviations used in the guide are defined below.

AIA	Authority Information Access
AOR	Authorized Organizational Representative
CA	Certification Authority
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Objects Registry
CSR	Certificate Signing Request
CSS	Certificate Status Server
DN	Distinguished Name
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS PUB	(US) Federal Information Processing Standards Publication
FPKI	Federal Public Key Infrastructure
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IS	Information System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
ISO	International Organization for Standardization
ITU-T	International Telecommunications Union – Telecommunications Sector
NIST	National Institute of Standards and Technology
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCSP	Online Certificate Status Protocol

OID	Object Identifier
OZ	Operations Zone
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PSS	Probabilistic Signature Scheme
PZ	Public Zone
RA	Registration Authority
RZ	Restricted Zone
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
RSASSA	RSA Signature Scheme with Appendix
SHA	Secure Hash Algorithm
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAZ	Special Access Zone
SP	Special Publication
SSP-REP	Shared Service Provider Repository Service Requirements
TAM	Trust Anchor Manager
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
U.S.C.	United States Code
UUID	Universal Unique Identifier
VPN	Virtual Private Network
WAP	Wireless Access Point

Appendix B—Glossary

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Anonymous	Having an unknown name.
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized as having the authority to verify the association of attributes to an identity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Authorized Organizational Representative (AOR)	A person (potentially among several) within an organization who is authorized to vouch for non-person identites. Any particular AOR is not permanently linked to any particular non-person identity; the CA must only ascertain that the AOR is legitimately associated with the organization, and that the AOR is identified as having authority for the identity in question.
Backup	Copy of files and programs made to facilitate recovery if necessary.

	[NS4009]
Bastion Host	A special purpose computer on a network specifically designed and configured to withstand attacks.
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term "certificate" refers to X.509 certificates that expressly reference the OID of this CP in the certificatePolicies extension.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a certification authority to perform certificate issuance and revocation.
CA Operating Staff	CA components are operated and managed by individuals holding trusted, sensitive roles.
Certificate Policy (CP)	A certificate policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A certificate policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of public key certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
CPS Summary	A publically releasable version of the CPS.
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a certification authority of the certificates that it has issued that are revoked prior to their stated expiration date.

Certificate Status Server (CSS)	A trusted entity that provides on-line verification to a relying party of a subject certificate's revocation status, and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cross-Certificate	A certificate used to establish a trust relationship between two certification authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS 140]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer’s digital certificate; and (2) whether the message has been altered since the transformation was made.
End Entity Certificate	A certificate in which the subject is not a CA.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.

Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Management Key	Key exchange, key agreement, key transport
Key Pair	Two mathematically related keys having the properties that (1) one (public) key can be used to encrypt a message that can only be decrypted using the other (private) key, and (2) even knowing the public key, it is computationally infeasible to discover the private key.
Key Rollover Certificate	The certificate that is created when a CA signs a new public key with an old private key, and vice versa
Modification (of a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a relying party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the Federal PKI, OIDS are used to uniquely identify certificate policies and cryptographic algorithms.
Online Certificate Status Protocol	Protocol which provides on-line status information for certificates.
Operations Zone (OZ)	Network area containing systems for routine business operations.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring on-line).

Policy Authority (PA)	Body established to oversee the creation and update of certificate policies, review certification practice statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
Privacy	Restricting access to subscriber or relying party information in accordance with Federal law.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Pseudonym	A subscriber name that has been chosen by the subscriber that is not verified as meaningful by identity proofing. [NS4009]
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is normally made publicly available in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public/private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Public Zone (PZ)	Network area that is not behind a protective boundary controlled by the organization.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a registration authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate that contains the new public key.
Relying Party	A person or entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Restricted Zone (RZ)	Controlled network area for sensitive data processing and storage
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a

	specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Security Auditor	An individual (e.g. employee, contractor, consultant, 3rd party) who is responsible for auditing the security of CAs or Registration Authorities (RAs), including reviewing, maintaining, and archiving audit logs; and performing or overseeing internal audits of CAs or RAs. A single individual may audit both CAs and RAs. Security Auditor is an internal role that is designated as trusted.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Special Access Zone (SAZ)	Highly controlled network area for processing and storage of especially high value data.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, an application or network device.
Superior CA	In a hierarchical PKI, a CA that has certified the certificate signature key of another CA, and that constrains the activities of that CA. (See subordinate CA).
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Trust List	Collection of Trusted Certificates used by relying parties to authenticate other certificates.
Trust Zone	The level of security controls in a network segment.
Trusted Agent	Entity authorized to act as a representative of a CA in confirming subscriber identification during the registration process. Trusted agents do not have automated interfaces with certification authorities.

Trust Anchor Manager	Authorities who manage a repository of trusted Root CA Certificates. They act on behalf of relying parties, basing their decisions on which CAs to trust on the results of compliance audits. A TAM sets requirements for inclusion of a CA's root public key in their store. These requirements are based on both security and business needs. The TAM has a duty to enforce compliance with these requirements, for example, requirements around the supply of audit results, on initial acceptance of a root, and on an ongoing basis. TAMs will follow their normal practice of requiring CAs to submit an annual audit report.
Trusted Certificate	A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. [NS4009]
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS 140]
Zone Boundary	The limit of authority over the security of the data processed within the boundary.

Appendix C—References

ABADSG — Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html

CABF Base — CA Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.1, 14 Sep 2012. https://www.cabforum.org/Baseline_Requirements_V1_1.pdf

CABF EV — Guidelines for the Issuance and Management of Extended Validation Certificates, version 1.4, 29 May 2012. https://www.cabforum.org/Guidelines_v1_4.pdf

CCP-PROF — X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program. http://www.idmanagement.gov/fpkipa/documents/CertCRLprofileForCP.pdf

CIMC — Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001. http://csrc.nist.gov/pki/documents/CIMC_PP_20011031.pdf

E-Auth — E-Authentication Guidance for Federal Agencies, M-04-04, December 16, 2003. http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

FIPS 140 — Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

FIPS 186-3 — Digital Signature Standard (DSS), FIPS 186-3, June 2009. http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf

FIPS 201-1 — Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201-1, March 2006. http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

FOIACT — 5 U.S.C. 552, Freedom of Information Act. http://www4.law.cornell.edu/uscode/5/552.html

ISO9594-8 — ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

ITMRA — 40 U.S.C. 1452, Information Technology Management Reform Act of 1996. http://www4.law.cornell.edu/uscode/40/1452.html

NAG69C — Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.

NSD42 — National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted

version)

NS4005 NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.

NS4009 NSTISSI 4009, National Information Systems Security Glossary, January 1999.

PACS *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.2, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, July 30, 2004. http://www.idmanagement.gov/smartcard/information/TIG_SCEPACS_v2.2.pdf

PKCS#1 Jakob Jonsson and Burt Kaliski, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, RFC 3447, February 2003. http://www.ietf.org/rfc/rfc3447.txt

PKCS#12 PKCS 12 v1.0: Personal Information Exchange Syntax-June 24, 1999. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf

RFC 2510 Certificate Management Protocol, Adams and Farrell, March 1999. http://www.ietf.org/rfc/rfc2510.txt

RFC 2560 X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP, Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams, June 1999. http://www.ietf.org/rfc/rfc2560.txt

RFC 2822 Internet Message Format, Peter W. Resnick, April 2001. http://www.ietf.org/rfc/rfc2822.txt

RFC 3647 Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003. http://www.ietf.org/rfc/rfc3647.txt

RFC 4122 A Universally Unique IDentifier (UUID) URN Namespace, Paul J. Leach, Michael Mealling, and Rich Salz, July 2005. http://www.ietf.org/rfc/rfc4122.txt

RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, D. Cooper etal, May 2008, http://www.ietf.org/rfc/rfc5280.txt

SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, NIST Special Publication 800-37, May 2004. http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf

SP 800-73-3 Interfaces for Personal Identity Verification – Part 1: End-Point PIV Card Application Namespace, Data Model and Representation, NIST Special Publication 800-73-3, February 2010. http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART1_piv-card-applic-namespace-date-model-rep.pdf

SP 800-88	NIST Special Publication 800-88: Guidelines for Media Sanitization http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf
SP 800-53	NIST Special Publication 800-53: Recommendation for Security Controls for Federal Information Systems and Organizations http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
SP 800-61	NIST Computer Security Incident Handling Guide, Rev 2. National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf
SP 800-57	NIST Special Publication 800-57 Rev 3, Recommendation for Key Management stpubs/800-61/sp800-61-revised2_Aug-2012.pdfndards and Technology http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf
SSP REP	Shared Service Provider Repository Service Requirements. Federal PKI Policy Authority Shared Service Provider Working Group, December 13, 2011. http://www.idmanagement.gov/fpkipa/documents/SSPrepositoryRqmts.doc
SP 800-147	NIST Special Publication 800-147, BIOS Protection Guidelines. April 2011. http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf
SP 800-147B	NIST Special Publication 800-147b, BIOS Protection Guidelines for Servers (Draft). July 2012. http://csrc.nist.gov/publications/drafts/800-147b/draft-sp800-147b_july2012.pdf